uc3m | Universidad Carlos III de Madrid

Grado en Tecnologías de Telecomunicaciones
2017/2018

Trabajo Fin de Grado

"Auditoría de seguridad en la red de Bitcoin"

Víctor Sindín García

Tutor

Marcelino Bagnulo Braun

Leganés, 2018

RESUMEN

Bitcoin es una divisa electrónica basada en una red de pagos P2P que opera al margen de cualquier autoridad central o banco. Esta criptomoneda utiliza por debajo la tecnología blockchain, un registro público que funciona mediante una base de datos distribuida con un sistema de codificación de información sofisticado que almacena el histórico de todas las transacciones realizadas, evitando así el mayor problema de las monedas digitales conocido como *double spending.* Cualquier usuario puede formar parte activa de la red, otorgando la transparencia de la que carecen los modelos basados en la confianza en terceros.

Esta tecnología ha supuesto sin duda una revolución sin precedentes en el ámbito económico-tecnológico en la última década desde su creación en 2008. Se trata de la creación de un sistema plural, transparente y democrático en el que prima la descentralización. En la actualidad ya existe el modelo de economía colaborativa explotado por empresas multinacionales como Airbnb, pero la innovación que incorpora la arquitectura blockchain es la ausencia de necesidad de plataformas intermediarias.

El principal objetivo del proyecto es estudiar el anonimato y la privacidad de esta criptomoneda, tanto a nivel de protocolo como de red. Se ha descargado el cliente completo Bitcoin Core en un servidor cedido por la universidad, lo cual ha permitido formar parte de la red de nodos verificadores de transacciones del blockchain. Esto nos permitirá obtener información de transacciones, bloques, además de direcciones IP entre pares. Posteriormente se propondrán y analizarán los servicios existentes para mitigar las carencias del protocolo a nivel de anonimato, como son los mezcladores (*mixers coins*) o el uso de la red TOR, con el objetivo de evitar el rastreo de transacciones y la identidad en una comunicación entre pares mediante técnicas de análisis de tráfico.

Por último, se propondrán otras criptomonedas alternativas que proporcionan una mayor privacidad, como Zcash con un sistema criptográfico conocido como pruebas de conocimiento cero (*Zero knowledge*) llamado *zk-SANRKS* que permite realizar transacciones anónimas, o Monero basada en una nula trazabilidad.

Palabras claves: Bitcoin, blockchain, criptomoneda, transacción, nodo

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

1.1 Motivación del Trabajo

El principal motivo del estudio de la tecnología y la posterior realización del trabajo viene dado por la necesidad conocer tanto el potencial de la misma como su funcionalidad. Hoy en día todavía hay mucho escepticismo entorno a la tecnología blockchain, tal vez por la continua especulación en el valor de las criptomonedas, lo que provoca un fuerte rechazo en la sociedad. Esto es debido a la volatilidad del valor monetario y a los numerosos intentos gubernamentales de llevar a cabo fuertes regulaciones con el fin de alejar las criptomonedas de actividades ilegales. Principalmente a día de hoy estas actividades más conocidas son lavado de dinero, financiación del terrorismo y adquisición de mercancía ilegal [1]. Esto provoca cierto temor y desconfianza entre los inversionistas, ya que estas medidas hacen peligrar el fundamento de la tecnología que es la descentralización.

A pesar de toda esta sombra de ilegalidad que ensombrece y acompaña a Bitcoin, la tecnología subyacente (blockchain) presenta una cantidad de posibilidades completamente nuevas a lo que hoy en día conocemos. Básicamente es una tecnología que ofrece la posibilidad de llevar a cabo transacciones entre pares de manera segura sin la necesidad de intermediarios para que arbitren en el proceso, además estas son públicas e irreversibles. Son muchas las organizaciones a nivel mundial que apuestan por la integración de esta tecnología, con gran presencia en asesoramiento fiscal, legal y financiero e incluso empresas como IBM han creado recientemente un nuevo departamento exclusivo para el desarrollo e integración de *blockchain* privadas.

Por otro lado, además de las ventajas que puede aportar al ecosistema financiero, gracias a los contratos inteligentes, que usan el *blockchain* como fuente de información, se puede aplicar a otras áreas de interés como el sistema sanitario, con la unificación del historial clínico de los pacientes en la cadena de bloques, un sistema único de patentes, un sistema de alquileres como Airbnb pero eliminando las comisiones impuestas por una tercera entidad mediadora que verifique que se cumplen los términos del contrato acordado entre pares, arrendador y arrendatario. Estamos presenciando una revolución tecnológica, una época de constante desarrollo e innovación en la que los ciclos de los modelos de negocio cada vez ensanchan más su margen de continua renovación, haciendo compleja la distinción de las tecnologías que van a prosperar y, por otro lado, las que no tienen cabida en el mercado.

1.2 Objetivos

En el presente Trabajo de Fin de Grado se ha realizado una auditoría de seguridad de sistemas de información sobre el *blockchain* y el protocolo Bitcoin. El principal objetivo de este estudio es ayudar a comprender qué nivel alcanza el anonimato proporcionado por la red y el riesgo al que se expone un usuario que hace uso de la tecnología.

Bitcoin a menudo se describe como una moneda anónima porque es posible enviar y recibir bitcoins sin dar ninguna información de identificación personal. Sin embargo, lograr un anonimato razonable con Bitcoin puede ser bastante complicado y el anonimato perfecto puede ser prácticamente imposible. Bitcoin es seudónimo. Enviar y recibir bitcoins es como escribir bajo un seudónimo. Si el seudónimo de un usuario alguna vez se vincula a su identidad, todo lo que se escribe bajo ese seudónimo será asociado a ellos.

En este trabajo se abordará la seguridad y el anonimato de Bitcoin desde tres niveles diferentes:

- Nivel de red: A pesar de que las direcciones IP no son almacenadas en el Blockchain de Bitcoin, en este trabajo se estudiará la forma de obtener las direcciones IP usadas en una transacción. Por un lado, si un usuario hace uso de un servicio de terceros (como un e-wallet o un *exchange*), un atacante con acceso a los *logs* del servicio web podría llegar a identificar las trazas del paqueteo, por otro lado, siendo esta última la que se estudiará en profundidad en este trabajo, existe la posibilidad de conectarse a nodos activos monitorizando a través del cliente Bitcoin Core.
- Transacción: Bitcoin es una moneda cuya trazabilidad se considera alta, es por eso que existen servicios como los *mixers* que intentan romper con las trazas reflejadas en el libro contable para aumentar su anonimato y evitar la trazabilidad de sus actividades. Con el fin de comprobar este hecho, se realizarán consultas a una base de datos SQL (*StructuredQueryLanguage*) en la que se encuentra almacenado todo el blockchain para obtener ciertos aspectos que podrían ser usados para inferir información privada del propietario.
- Monedero: Existen diversos tipos de monederos para almacenar los Bitcoin, cada una de ellas aporta un nivel de seguridad y complejidad diferente, por lo que usualmente son objetivo de la mayor parte de ataques en el sistema, ya que es la única parte cuya seguridad es independiente del protocolo Bitcoin en sí. Concretamente se analizará la seguridad de la cartera del cliente y diversas formas en las que un atacante puede hacerse con las claves del monedero y así, hacer uso de los fondos del mismo.

2. GESTIÓN DEL PROYECTO

2.1 Planificación temporal

Con el fin de mejorar la visibilidad de las fases de trabajo, en esta sección se lleva a cabo la planificación temporal del proyecto final de carrera mediante un diagrama de Gantt, el cual realiza un desglose de las fases y las tareas de las que consta el proyecto. El diagrama de Gantt es una herramienta que pretende representar de manera visual en desarrollo temporal de la vida de un proyecto mediante el uso de gráficas. Las fases del trabajo vienen representadas mediante barras horizontales que representan el inicio y el fin de la fase, junto con la compatibilidad entre tareas, es decir, si hay fases del proyecto que se pueden solapar o son dependientes, por lo que una tarea necesita que termine su predecesora para poder comenzar.

En este trabajo se ha optado por un hilo temporal relativamente consecutivo, donde se puede apreciar que no se produce apenas solape entre tares, y esto es así debido al carácter individual que tiene el proyecto y a la necesidad de asimilación de conceptos antes de seguir con la investigación teórica del siguiente concepto, como puede apreciarse en la *ilustración 2*.

En el eje vertical del diagrama de encuentran el desglose analítico de las tareas, para las cuales se ha empleado la herramienta *Proyect Libre,* un software gratuito que genera este tipo de diagramas. En total en el proyecto se han realizado 10 tareas con una duración total de 175 días (5 meses, 2 semanas y 1 día), dando comiendo el lunes 2 de abril de 2018 y finalizando el lunes 17 de septiembre del mismo año. Asumiendo una media diaria de trabajo de 2,5 horas de lunes a jueves, 4 horas los viernes debido a la jornada reducida del trabajo y 6 horas dedicados el fin de semana. Teniendo en cuenta la segregación de horas anterior, la media de horas al día es de 4,42 horas, lo que equivale a 33 horas semanales. Esto hace un total de 481,78 horas destinadas al proyecto.

Como resultado de la *ilustración 1* y partiendo de la definición del diagrama de Gantt, se muestra una representación temporal de todas las fechas asociadas a sus correspondientes tareas, tal y como se observa en el diagrama de la *ilustración 2*.

	Inicio del Trabajo de Fin de Grado	1 day?	2/04/18 8:00	2/04/18 17:00
	Planificación	126 days?	**2/04/18 8:00**	**24/09/18 17:00**
	Estudio del protocolo Bitcoin	33 days?	2/04/18 8:00	16/05/18 17:00
	Análisis del blockchain	7 days?	16/05/18 8:00	24/05/18 17:00
	Estudio de la arquitectura de red	5 days?	24/05/18 8:00	30/05/18 17:00
	Ejecución	84 days?	**30/05/18 8:00**	**24/09/18 17:00**
	Instalación del cliente Bitcoin-Core	12 days?	30/05/18 8:00	14/06/18 17:00
	Análisis de datos	14 days?	11/06/18 8:00	28/06/18 17:00
	Análisis de vulnerabilidades	9 days?	28/06/18 8:00	10/07/18 17:00
	Pruebas	11 days?	10/07/18 8:00	24/07/18 17:00
	Interpretación de resultados	4 days?	24/07/18 8:00	27/07/18 17:00
	Documentación	61 days?	**2/07/18 8:00**	**24/09/18 17:00**
	Redacción de la memoria	37 days?	2/07/18 8:00	21/08/18 17:00
	Preparación de la presentación	6 days?	17/09/18 8:00	24/09/18 17:00
	Fin del Trabajo de Fin de Grado	0 days?	24/09/18 8:00	24/09/18 8:00

Ilustración 1 Fecha y duración evaluada para cada tarea

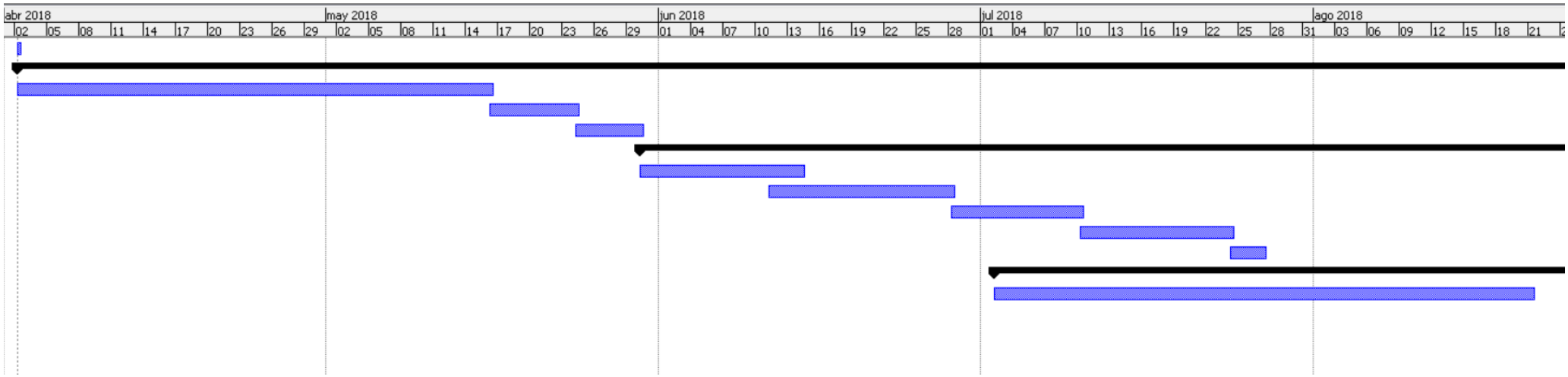


Ilustración 2. Gráfico del diagrama de Gantt

2.2 Presupuesto

Se llevará a cabo un análisis de los costes totales del Trabajo Fin de Grado, los cuales se fraccionan en dos grupos principalmente, *directos* (personal y material) e *indirectos* (20% de los costes directos). Para el cálculo del presupuesto, se han utilizado los conocimientos adquiridos en el curso "Taller de Finanzas para ingenieros" acreditado por la Universidad Carlos III junto con los de la asignatura de gestión empresarial.

- Costes directos: gastos relacionados con obtención de productos o realización de servicios [55]. Se divide en:
    - Costes de personal: en función del grado, la experiencia y la situación geográfica del trabajador. Según un estudio realizado, un ingeniero con menos de 4 años de experiencia recibe un salario medio de 25.000€ brutos/año [56], trabajando aproximadamente 40 horas semanales. El empresario debe pagar los impuestos en base a la cotización del país en la que se encuentra, seguridad social (contingencias comunes) y otros conceptos de recaudación conjunta y aportaciones, como son el desempleo, la formación profesional, el fondo de garantía social, los accidentes laborales y las enfermedades profesionales [57]. A continuación, en la *tabla 1*, se mostrarán las cantidades a pagar para la realización de este Trabajo Fin de Grado. Todos los datos están ajustados a los tiempos de realización del trabajo. Además, para calcular el coste del trabajador se empleará la fórmula:

$$Horastrabajadas = Díastrabajados \cdot Horadía$$

$$Coste = Horastrabajadas \cdot Preciohora$$

Tabla 1. Costes de personal.

	TRABAJADOR			*EMPRESARIO*				
Personal	Días trabajados	Horas día	Horas totales dedicadas	Contingencias comunes 23.6%	Contingencias profesionales y conceptos de recaudación conjunta 8.85%	Coste total personal	Precio hora/día	Coste
Víctor Sindín García	109	4,42	**481,78**	5.100	1.824,23€	24.450 €	**15€/hora**	7.226,7€

- Costes de material: hace referencia a la inversión inicial tanto en software como en hardware para la realización completa del proyecto, en ellos se todo el material que ha sido utilizado para la realización del Trabajo Fin de Grado [56]. En *tabla 2* se encuentra especificado con detalle el material usado. En la *tabla 3*, se muestran los costes de software.

Producto	*Precio*
Ordenador portátil	799€
Smartphone	150€
Cable USB	2,25€
Pantalla externa BENQ	139€
Ratón	14,99€
Teclado	60€
Servidor UC3M (350 Gb)	0€
TOTAL	1.165,24€

Tabla 2. Coste del material hardware

Producto	*Precio*
Paquete de Microsoft Office 2013	174,99€
Bitcoin Password (Thegrideon Software)	29,95€
Bitcoin Core	0€
Note Pad ++	0€
Windows 10 (Licencia UC3M)	0€
Sublime Text 3	0€
ProjectLibre	0€
TOTAL	234,09

Tabla 3. Coste del material software

En el momento de adquirir el material necesario para la realización del proyecto hay que realizar una estimación su vida útil, es decir, la devaluación anual que tiene un activo, concepto acuñado bajo el término de amortización lineal o de cuotas fijas. Cabe destacar que hay otros tipos de amortización, pero en este proyecto se aplicará la mencionada ya que se entiende que el degaste será ligero pero constante con el paso del tiempo. Se estimará la amortización de los productos con respecto al tiempo de duración del proyecto [57]. Para calcular la amortización lineal la fórmula utilizada es la siguiente:

$$Amortización = \frac{Tiempo\ utilizado}{Tiempo\ de\ vida\ útil} \cdot Valor\ de\ adquisición \cdot Coeficiente\ (\%)$$

Donde:

- Tiempo utilizado: tiempo en el que se ha realizado el proyecto.
- Tiempo de vida útil: Normalmente tasado en horas de duración, Por lo general la vida útil de un producto son 5 años, equivalente a 60 meses. Este cambio de años a meses se lleva a cabo para igualar unidades y llevar a cabo el cálculo correctamente.
- Valor de adquisición: es el coste de los productos mostrados en la *tabla 2 y 3*.
- Coeficiente (%): es el porcentaje de uso que se dedica al proyecto, generalmente es el 100%.

Producto	*Coste*	*Coeficiente (%)*	*Duración del proyecto (meses)*	*Vida útil de un producto (meses)*	*Amortización lineal*
Ordenador portátil	799€	100	5,02	60	90,13
Smartphone	150€	100	5,02	60	12,88
Cable USB	2,25€	100	5,02	60	0,19
Ratón	34,99€	100	5,02	60	3,00
Teclado	60€	100	5,02	60	5,15
Paquete de Microsoft Office 2013	174,99€	100	5,02	60	15,02
Bitcoin password	29,99€	100	5,02	60	5,07
TOTAL					143,37

Tabla 4. Amortización de los activos

Por último, en la *tabla 5*, se muestra el montante total de los costes directos:

Tipo de costes directos	*Presupuesto*
Costes de personal	7226.7€
Costes de material Hardware	1.165,24€
Costes de material Software	234,09€
Amortizaciones	143,37€
Total sin IVA	8.769,40€
Total con IVA (21%)	10.610,97€

Tabla 5. Resumen del total de los costes directos.

- Costes indirectos: este tipo de coste, aunquetambién interfiere en la producción de un proyecto, no se pueden retribuir a cada uno de los productos de forma directa. Para poder calcularlo, se establece en el 20% del valor total de los costes directos. De esta manera, el valor total de los costes indirectos asciende a la cantidad de 2.350,99€.

En la siguiente tabla se resume el presupuesto final de este Trabajo Fin de Grado.

Tipo de costes	*Presupuesto*
Costes directos	10.610,97€
Costes indirectos	2.122,19€
TOTAL	12.733,16€

Tabla 6. Resumen de los costes

Por tanto, el presupuesto total del proyecto es de 12.733,16€.

2.3 Marco regulador

La descentralización de un sistema se basa una confianza total entre pares desconocidos lo cual es posible gracias a la transparencia total de la cadena de bloques, anulando así la necesidad de una entidad central e imparcial que regule el sistema, siendo esta una de las características principales de esta tecnología. Debido a trascendencia tecnológica en pleno auge de la "Era Digital" y a la gran repercusión social, las grandes organizaciones gubernamentales han decidido mediar y posicionarse.

En el ámbito nacional, la Agencia Tributaria publica en el BOE (23/01/2018) el "Plan de Control Tributario y Aduanero" en el que se realiza un estudio de la incidencia fiscal de nuevas tecnologías, como el *blockchain* [6]. El Órgano Centralizado de Prevención del Blanqueo de Capitales del Consejo General del Notario (OCP) propone como medida contra el lavado de dinero una modificación de la Directiva Europea contra el blanqueo de capitales [5], donde se pide a las sociedades intermediarias un registro más exhaustivo mediante documentos oficiales nacionales donde se pueda obtener un registro canónico de las personas que hacen uso del servicio.

La actualidad en la legislación aplicable es todavía precaria y las regulaciones que se empiezan a llevar a cabo en distintos países son aún rudimentarias, debido a que es una tecnología primeriza en la que se siguen estudiando posibles impactos, aplicaciones y riesgos.

Las criptomonedas se rigen por las actuales regulaciones de protección al consumidor o las regulaciones vigentes de organismos que persiguen el blanqueo de capitales y, mientras que en países como China o Islandia han restringido su uso, en el resto de países no hay consenso unilateral. A continuación, se realizará un desglose del actual margen regulador en distintas regiones donde podremos observar una comparativa de la disparidad legislativa sobre el blockchain que rige en la actualidad [8].

Estados Unidos, cuna del desarrollo tecnológico en la actualidad, no tiene una legislación vigente unilateral y, sin embargo, ya han surgido leyes y regulaciones sectoriales sobre algunos servicios y transacciones basadas en blockchain. Se ha definido una "Red de Ejecución de Delitos Financieros ", donde las empresas que trabajen con criptomonedas deben inscribirse. Las compañías que ofrecen servicios de compra venta de monedas como "Coinbase" o "Coinmama" están expuestas a la ley anti lavado de dinero, es decir, exigen a los usuarios un registro en la plataforma donde cada vez que quieres realizar unas operaciones debes identificarte. También aplican la ley de secreto bancario, la cual se podrá aplicar de manera directa si se desea obtener información sobre un usuario que transfiera dinero.

La Unión Europea avala el uso del blockchain, cuyos principales temas a tratar en la agenda europea son la transparencia y la seguridad. Consecuencia de ello es la creación del proyecto Blockchain4EU, un laboratorio de Políticas de la UE donde un grupo de expertos evalúa los marcos reguladores de los estados miembros para elaborar una respuesta coordinada. De hecho, en muchos de los estados miembros no existe aún una regulación específica sobre las criptomonedas; es el caso de El Banco Central Europeo (BCE), que ha dejado clara su postura y no considera las criptomonedas equivalentes al dinero, alegando que en caso de pérdida o fraude no existe una organización o mecanismo de rescate.

A finales del año 2017, la UE acuerda las enmiendas propuestas a la cuarta directiva anti lavado de dinero (4AMLD) introduciendo una serie de reformas para acercar a los proveedores y administradores de servicios criptográficos a esta entidad, y así prevenir y denunciar el lavado de dinero y la financiación del terrorismo ilegal [8].

Islandia prohíbe el comercio exterior de Bitcoin a pesar de que alberga importantes instalaciones mineras del protocolo. En 2013, el gobierno islandés emitió una declaración prohibiendo el comercio exterior con Bitcoin, lo que no prohíbe a sus ciudadanos poseerlo o usarlo dentro de Islandia, u obtenerlas por minería de blockchain.

China es el país más pionero en la investigación de blockchain y la tecnología de las criptomonedas a través de organismos como el "Bando Popular de China" (PBOC), que llevan investigando desde el año 2014. En 2016, lanza un proyecto llamado "plataforma de comercio digital de papel comercial" para testear la tecnología, llegando a establecerse en 2017 el "Instituto de Investigación de Monedas Digitales" y emitiendo una moneda digital legal en esta plataforma durante un periodo de prueba [6].

Pese a las importantes investigaciones sobre la tecnología y albergar las mayores instalaciones de minado de criptomonedas, las regulaciones nacionales han prohibido el uso comercial del Bitcoin como moneda de curso legal. En 2017, se prohíben los *exchanges* y las actividades financieras relacionadas con monedas digitales mediante instituciones de pago financieras o no bancarias.

Japón se convierte en 2017 en el primer país en admitir el Bitcoin como moneda de curso legal. La "Agencia de Servicios Financieros" (FSA) es el organismo encargado de hacer cumplir las regulaciones, dando respaldo legal a los *exchanges* que ofrecen monedas virtuales.

2.4 Entorno socio económico

La aceptación por parte de la sociedad del sistema blockchain puede desembocar en un nuevo nivel de maduración en la forma en la que se entiende el gobierno, la autoridad, la independencia y el grado de implicación. No es habitual que el gobierno sea una responsabilidad personal y hoy en día no se entiende un sistema de igual a igual con una autoridad política autónoma descentralizada, en contraste con la imposición de una institución externa centralizada. La sociedad no está acostumbrada a muchos de los aspectos de la tecnología Bitcoin, como el hecho de tener que hacer copias de seguridad del dinero; sin embargo, cuando adoptamos nuevas tecnologías aprendemos nuevos comportamientos y conceptualizaciones.

La sociedad ha madurado hasta el entendimiento de una autoridad descentralizada en otros contextos, como es el caso de la industria de la información, en la que se ha producido una gran metamorfosis digital donde noticias y publicaciones han quedado descentralizadas con los blogs y redes sociales, lo que provocó la reestructuración de la industria de los medios de comunicación. El entretenimiento sufrió una transformación similar, con la coexistencia de grandes medios corporativos como los canales de *YouTube*, donde particulares suben su propio contenido a la red, o el consumo masivo de *Netflix*, portal multimedia donde el usuario elije el contenido que desea visualizar. La cadena de valores ha cambiado y ahora es el usuario quien tiene la posibilidad de elegir el contenido que quiere consumir, en base a sus propios criterios.

Otro desafío destacado, tanto funcional como técnico, está relacionado con los modelos comerciales. Al principio, los modelos de negocio tradicional podrían no ser aplicables a Bitcoin, ya que el objetivo de los modelos descentralizados entre pares es que no hay intermediarios que faciliten una tarifa de transacción, como suceden en el modelo comercial básico. Sin embargo, todavía hay muchos productos y servicios rentables que generan ingresos en la nueva economía blockchain. La educación y el acercamiento de las herramientas al usuario son necesarias, al igual que mejorar la eficiencia de toda la infraestructura bancaria. De cara al futuro, la reconfiguración de todos los negocios y el comercio con *smartcontracts* (contratos inteligentes) puede ser complejo y difícil de implementar; aun así, surge una oportunidad de negocio para proveedores de servicios que ofrezcan implementación, educación al cliente, establecimiento de estándares y otras utilidades de valor agregado [23]. Algunos tipos de modelos comerciales que se han desarrollado con software empresarial y computación en la nube también podrían ser aplicables a la economía de Bitcoin. Otro modelo de negocio que surge es auditar los contratos inteligentes, para confirmar que los contratos inteligentes de IA (inteligencia artificial) que se ejecutan en el blockchain estén cumpliendo las instrucciones programadas.

2.5 Impacto medioambiental

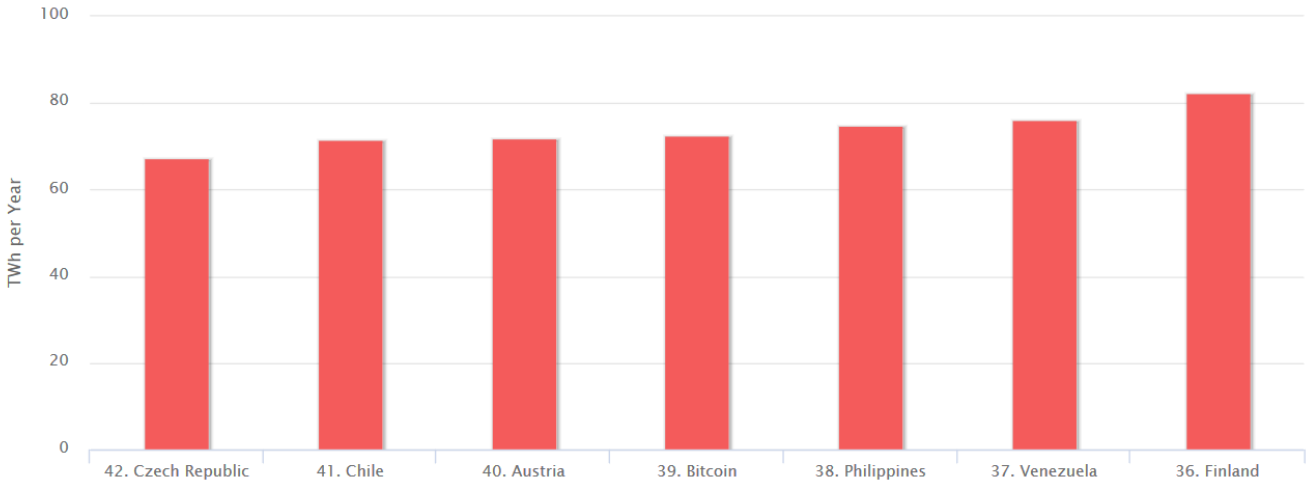
La electricidad invertida en el proceso de minado de Bitcoin se ha convertido en un serio tema de debate en los últimos años. El sistema criptográfico de "*proof-of-work"* (prueba de trabajo) requiere una gran cantidad de cálculos de *hash* para el proceso de validación de transacciones sin intermediarios, denominado *peer-to-peer*. El proceso de producir un bloque válido está basado principalmente en el" prueba y error", donde los mineros realizan numerosos intentos para calcular nuevos *hashes* con el fin de encontrar el valor correcto de un componente del bloque llamado *nonce*. La cantidad de intentos por segundo viene dada por el *hashrate*, es decir, la potencia de procesamiento del minero, que depende del equipo de utilizado, y cuya unidad de medida se expresa usualmente en *GH*/s (*Gigahashes* por segundo, equivalente al cálculo de mil millones de *hashes* por segundo) [18]. Finalmente, los mineros comprueban si el bloque completo resultante de esta operación cumple con los requisitos impuestos por el protocolo, ya que no hay manera alguna de predecir el resultado. El primer minero en sellar el bloque, es decir, en encontrar el *nonce* correcto, es recompensado con una cantidad determinada de BTC, junto a las tarifas correspondientes a las transacciones procesadas en el nuevo bloque.

Debido a que la minería puede proporcionar una corriente sólida de ingresos, la gente está dispuesta a utilizar máquinas con un gran *hashrate* que, por consecuencia, consumen gran cantidad de energía. Con el transcurso de los años la minería ha dejado de ser rentable ya que la dificultad del acertijo criptográfico ha aumentado a tal punto que un individuo particular no obtiene ningún beneficio neto, surgiendo así grandes asociaciones colaborativas de minado denominadas "pools de minado", o grandes superficies industriales repletas de dispositivos destinados al minado (ASICS), denominadas "granjas" donde se suma el poder computacional de todos los participantes, llevando a cabo un minado distribuido.

Ilustración 1. Granja de minado en China [19]

El consumo total de energía de la red de Bitcoin ha ido aumentando en proporciones épicas ya que, además del gasto energético obvio, el minado también induce a otros gastos indirectos como pueden ser los mecanismos de refrigeración para bajar la temperatura de los dispositivos y evitar su sobrecalentamiento. Por esto, se ha acometido una gran inversión de dinero destinado al minado en localizaciones como Islandia, que posee el precio más barato de Europa, estableciéndose en 0,103 € por kWh [21], y con un gélido clima que requiere una menor inversión en servicios de refrigeración. Según un informe publicado por la Agencia Internacional de la Energía ("*Key WorldEnergyStatics 2017*") [20], toda la red de Bitcoin ahora consume más energía que ciertos países como muestra la siguiente gráfica.

Ilustración 2. Consumo energético en TW/h. [18]



El principal problema de Bitcoin reside en que la mayor parte del consumo energético de la red pertenece a China, la cual utiliza como materia prima el carbón, disponible a precios muy bajos en el país. Actualmente, existen otras alternativas a este problema que cada vez se agrava más, como el uso de energías renovables o utilizar otros algoritmos de prueba de trabajo de mayor eficiencia energética, como *proof-of-stake,* en el que los propietarios de las monedas crean los bloques, en lugar de los mineros, por lo que no se requieren máquinas que consuman tantos *hashes* por segundo y la energía consumida sea insignificante comparado con el *proof-of-work*.

Para poner en perspectiva la energía consumida por la red de Bitcoin, podemos compararla con otro sistema de pago como VISA. Según este método, la compañía consumió un total de 674,922 GJ [18] a nivel mundial para todas sus operaciones, en un desglose de 111.2000 millones de transacciones en 2017. Con los datos expuestos anteriormente, es posible demostrar que Bitcoin consume más energía por transacción que VISA, como se compara visualmente en el siguiente gráfico.

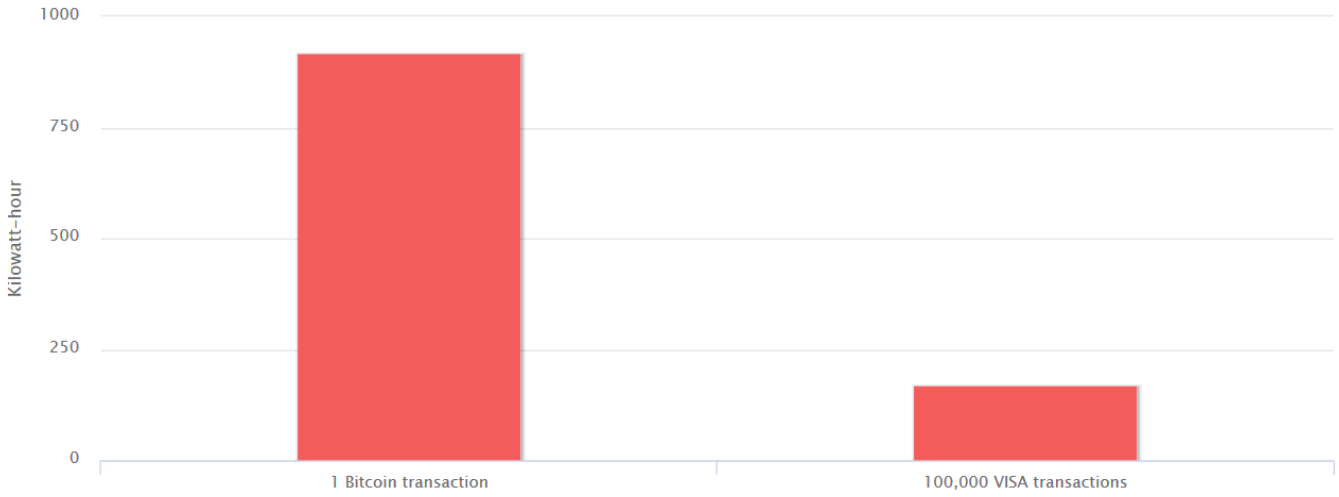


Ilustración 3. Comparativa de la red de Bitcoin versus el consumo medio de la de VISA

3. ESTADO DEL ARTE

3.1 Historia de las criptomonedas

Desde los inicios del comercio, la sociedad ha ido reinventado nuevas formas de intercambiar bienes y servicios. En su comienzo la necesidad de cubrir las necesidades básicas dio lugar al trueque, donde se intercambiaba directamente una mercancía que se disponía en exceso por otra. El principal problema de este sistema era la relatividad del valor que se le asignaba a los bienes en el momento del intercambio.

Posteriormente se usaron bienes específicos y con valores considerables como oro, sal, cacao o especias, lo que dio solución al problema de la subjetiva tasación de los bienes que existía anteriormente. Sin embargo, esta mercancía tenía como principal inconveniente su transporte, por lo que se empezaron a usar pepitas de oro, plata y cobre para realizar las transacciones, aunque era complicado saber el valor exacto del material.

A finales de la edad media se inventaron las primeras monedas con metales preciosos, la denominada tercera generación, que traían grabado un valor en función a su peso y tamaño. En 1661, un banco sueco emitió los primeros billetes, que no eran más que la representación monetaria del oro del que disponía.

La aparición de las monedas y billetes supusieron un gran avance ya que su uso era sencillo y resolvía el problema de la disponibilidad, aunque, por otro lado, surgieron problemas con el fraccionamiento, las falsificaciones y el transporte seguro. Entonces se precisó otra forma de hacer transacciones y comenzó el desarrollo de las operaciones electrónicas, dando lugar a la aparición de las tarjetas de débito y crédito. La primera permite comprar bienes y servicios transmitiendo los fondos de una cuenta a otra, mientras que la segunda permite comprar bienes y servicios transfiriendo fondos provenientes de un préstamo que tiene el consumidor en un banco a la cuenta del comercio. También surgió la billetera móvil, que permite guardar y transferir dinero, bienes y servicios operando directamente desde el móvil asociado a una cuenta bancaria personal.

En la última década del siglo XX, debido al aumento exponencial de las transacciones electrónicas y el auge del movimiento criptográfico, apareció la primera moneda electrónica desarrollada mediante DigiCash, una corporación dedicada a la investigación de dinero digital, siendo la primera en conseguir transacciones anónimas gracias a un protocolo criptográfico desarrollado por su fundador David Chaum, científico informático que puso los pilares del sistema de pagos anónimos basados en dinero digital como demuestra su documento publicado en 1982,

"BlindSignaturesforUntraceablePayments". En 1994 la compañía realizó la primera transacción electrónica**. [**9]

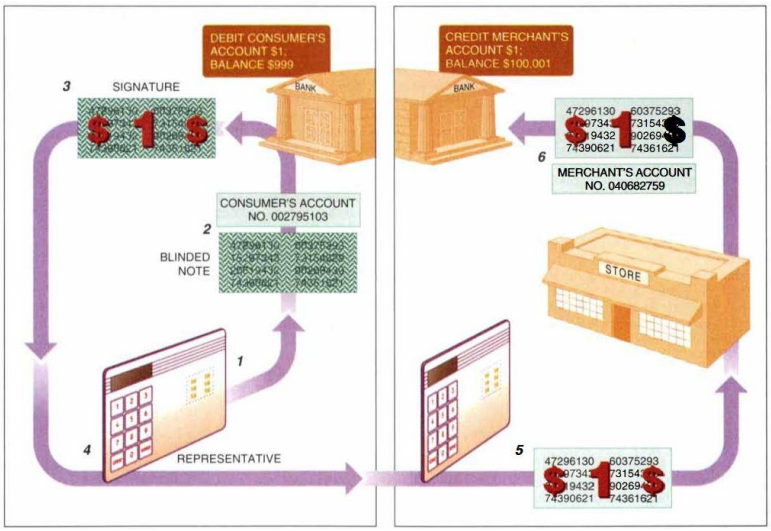


Ilustración 4. Primera transacción anónima [6]

Por último, en 2008, en plena crisis económica se publica un artículo bajo el nombre de "Bitcoin P2P e-cash paper" [10] en el que se presenta una nueva moneda digital, descentralizada y anónima, el Bitcoin. Satoshi Nakamoto, pseudónimo en el que se enmascara el desconocido autor del paper, utiliza como herramienta criptográfica la firma digital (SHA-256) y un sistema de validación de transacciones conocido como *proof-of-work*. Posteriormente, han aparecido otras criptomonedas que han intentado resolver las carencias que se han ido encontrado en Bitcoin como Ethreum, Ripple, Litecoin, etc.

3.2 Protocolo Bitcoin

Todo sistema financiero vigente en la actualidad está basado en una entidad central en la que se deposita la confianza en el momento de realizar pagos electrónicos, derivando en un pre incremento en el coste de la transacción. Estos costes, y la necesidad de confiar en una tercera persona imparcial se evitan cuando se usa dinero físico. Bitcoin es una moneda digital que está basada en una red de pago P2P con la ausencia de una autoridad central que no regula la emisión de la moneda ni pone restricciones a las operaciones, a diferencia de las monedas convencionales. Esta red se mantiene gracias al *blockchain*, una especie de libro contable público donde es posible consultar todas las operaciones realizadas. Esto se consigue a través de dos elementos criptográficos

fundamentales: las funciones *hash* (huella digital) y el sistema de firma digital basado en las claves pública y privada. [11]

Al igual que cualquier otra tecnología emergente, el uso de Bitcoin presenta ciertos beneficios y desafíos, a la par que riesgos asociados a su uso. Bitcoin tiene las siguientes características [24]:

- *Descentralizado:* ninguna autoridad central puede manipular o incautar la moneda ya que cada transferencia de criptomonedas sucede entre pares de igual a igual, de manera análoga al dinero en efectivo.
- *Anonimato y transparencia:* a menos que los usuarios de Bitcoin publiquen las direcciones de sus billeteras públicamente, es extremadamente difícil rastrear las transacciones hacia ellos. Sin embargo, incluso si las direcciones se hicieron públicas, se puede generar fácilmente una nueva dirección de billetera. Esto aumenta enormemente la privacidad respecto a los sistemas monetarios tradicionales, donde las terceras partes pueden acceder fácilmente a datos financieros personales. Además, este alto anonimato se logra sin renunciar a la transparencia del sistema, ya que todas las transacciones de Bitcoin están documentadas en un libro público.
- *Sin impuestos y tasas por transacción bajas:* debido a los dos puntos anteriores no existe una forma viable de implementar un sistema de tributación de Bitcoin. En el pasado, Bitcoin proporcionaba transacciones instantáneas casi sin coste, e incluso ahora tiene costes de transacción más bajos que una tarjeta de crédito, PayPal o transferencias bancarias.
- *Mecanismos resistentes frente a robo:* el robo de Bitcoins no es posible hasta que el adversario tenga las claves privadas, asociadas con el monedero del usuario. En particular, Bitcoin proporciona seguridad por su propio diseño; por ejemplo, a diferencia de las tarjetas de crédito, no expones tu clave privada cada vez que realizas una transacción. La transacción no puede ser revertida dado que la dirección de propiedad de los BTC enviados se cambiará al nuevo propietario.

Debido a la juventud de la tecnología todavía quedan muchos retos para poder mejorarla, entre otros reducir el alto consumo de energía, ya que la cadena de bloques usa el modelo PoW para lograr un consenso distribuido en la red, (aunque el uso de este modelo hace que la minería sea un proceso más resistente a diversas amenazas de seguridad) el consumo energético y los recursos informáticos empleados son muy altos. En particular, el procesamiento de una transacción de Bitcoin consume mayor energía que el uso de una tarjeta de crédito VISA, como se ha contrastado anteriormente en el gráfico reflejado en la *ilustración 3*. Mejorar este aspecto es necesario para garantizar el futuro de la tecnología.

Por otro lado, ya que no hay un tercero de confianza, si un usuario pierde la clave privada asociada con su billetera ya sea por un fallo en el disco duro, un virus o se pierde el dispositivo que almacena la llave, los BTC quedarán "huérfanos" en el sistema. Además, el anonimato proporcionado por el sistema Bitcoin fomenta la delincuencia cibernética para realizar diversas actividades ilícitas como *ransomeware* [43], el famoso "*WannaCry"* (ataque llevado a cabo el 12 de mayo de 2017 a nivel mundial que afectó a algunas de las empresas españolas más importantes como Telefónica, Iberdrola y Gas Natural), evasión de impuestos, mercado negro o lavado de dinero. De acuerdo con el análisis de riesgos realizado por M. Kiran y M. Stannett [44], el riesgo en el protocolo Bitcoin es alto, como en cualquier moneda virtual, provocando cierta desconfianza debido a la incertidumbre y el desconocimiento social. Los riesgos principales mencionados en este artículo son los siguientes.

- *Riesgos legales:* vienen dados por la oposición a reglas y regulaciones. Este riesgo también incluye la aplicación de la ley para operaciones financieras, operaciones, protección y seguridad del cliente ante infracciones que surgen como consecuencia del sistema Bitcoin.
- *Riesgos económicos:* deflación, volatilidad y problemas de tiempo para encontrar un bloqueo que pueda llevar a los usuarios a migrar hacia otra moneda que ofrezca servicios más rápidos.

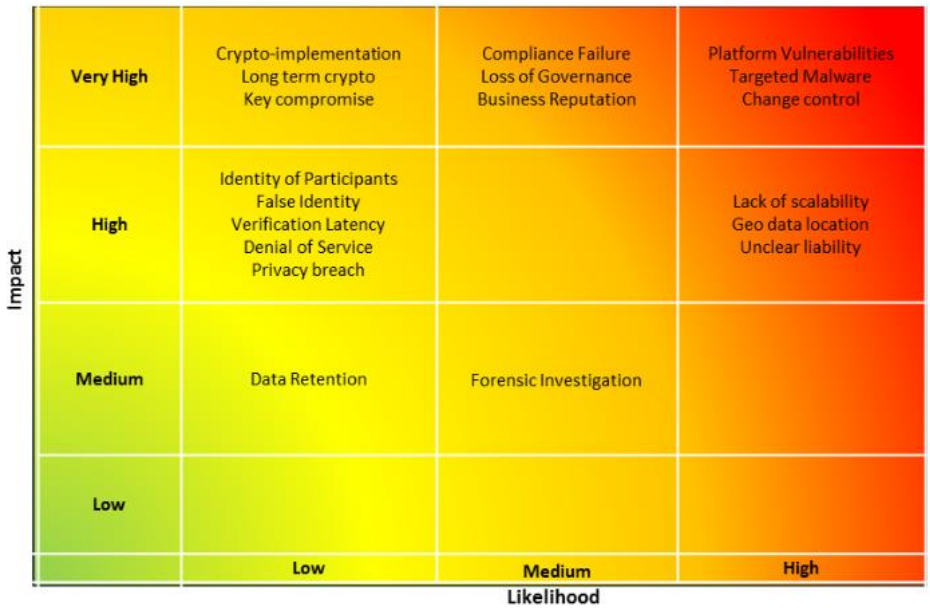


Ilustración 5. Riesgos y blockchain [46]

En 2016 se publica un artículo titulado “What motivates people to use bitcoin?” [45], donde se analiza la opinión social sobre el uso de bitcoins. Los usuarios argumentan que la mayor barrera para el uso de bitcoins es la falta de apoyo por parte del gobierno. Además, consideraron que los bitcoins deben ser aceptados como una moneda legítima y de confianza, y expresaron que el sistema debe proporcionar apoyo para realizar transacciones sin temor a la explotación criminal. Una minoría expresó su desconfianza sobre la manipulación de la cadena de bloques, opinión apoyada por el dato sobre la gran cantidad de pérdidas incurridas por los usuarios: “around 22,5% of the participants reported having lostt heir bitcoins due to security breaches”.

3.2.1 Estructura de la red

Bitcoin utiliza una red no estructurada punto a punto (P2P) basada en conexiones TCP no encriptadas. Este tipo de red es la idónea para Bitcoin, ya que el objetivo es distribuir información lo más rápido posible para llegar a un consenso sobre la cadena de bloques. Sin embargo, experimentar con el protocolo Bitcoin plantea un desafío.

Los nodos de Bitcoin mantienen una lista de direcciones IP de pares potenciales, y la lista se inicia a través de un servidor DNS, y las direcciones adicionales se intercambian entre pares. Cada par pretende mantener un mínimo de 8 conexiones TCP no cifradas. Por defecto, la conexión entre los pares se realiza en el puerto 8333 para conexiones entrantes. Cuando un par establece una nueva conexión, se lleva a cabo una negociación de manera segura con “*Layerhandshake”.* Los mensajes incluyen una marca de tiempo, direcciones IP y la versión del protocolo. Un nodo selecciona sus pares de forma aleatoria y un nuevo conjunto de pare después de una cantidad fija de tiempo. Esto se hace para minimizar la posibilidad y los efectos de un ataque “*netsplit”*, en el cual un atacante crea una vista incoherente de la red y la cadena de bloques en el nodo atacado. Desde la versión 0.7 de Bitcoin es compatible con IPv6. Con el objetivo de detectar cuando dos pares se han ido, Bitcoin utiliza una técnica que consiste en lo siguiente: si han pasado 30 minutos desde la última vez que se intercambiaros mensajes entre vecinos, los compañeros transmitirán un mensaje de saludo para mantener la conexión viva.

Los mineros conectados a la red reciben constantemente nuevos anuncios que informa del sellado de un nuevo bloque y dicha información se intercambia a través de la red mediante mensajes que contienen el *hash* del bloque minado. Si un minero descubre que no contiene en su registro el hash del bloque anunciado recientemente, transmite un mensaje de “GETDATA” a uno de sus vecinos. El vecino responde enviando la información solicitada en un bloque. En caso de que el bloque solicitado no llegue en 20 minutos, el minero desencadena la desconexión de ese vecino en particular y solicita la información de otro vecino.

La propagación de las transacciones ocurre en una secuencia de transacciones conocida como INV, GETDATA y TX de mensajes, en los cuales los nodos anuncian, solicitan y comparten transacciones que aún no se han incluido en el blockchain. Para establecer el consenso distribuido, las transacciones y los bloques creados recientemente se propagan a través de una técnica denominada "*flooding"* o inundación, es decir, se propaga a todo nodo vecino y así recursivamente, en toda la red. Los mineros almacenan nuevas transacciones para fines de minería, pero después de un tiempo los borran. Es responsabilidad del originador de la transacción que sea recibida por todos los nodos de la red. Para este fin, el minero podría necesitar retransmitir la transacción si no consigue entrar en la cadena de bloques al primer intento. Esto sirve para asegurar que la transacción sea considerada válida e incluida en el siguiente bloque.

3.2.2 Direcciones Bitcoin

Las direcciones en BTC hacen referencia a una cadena de dígitos alfanuméricos, entre 27 y 34 caracteres de longitud (por ejemplo: 1PZ5THirpbwtjklv1zCHCYFnxTxCPrVhk), la cual se genera de manera individual, sin ninguna entidad central que controle la creación de direcciones, por lo que en un caso hipotético podría suceder que dos usuarios diferentes hayan generado la misma dirección. El número de direcciones distintas que pueden existir en la red BTC es de 2^{160}, por tanto, la probabilidad de que coincidan dos direcciones públicas procedentes de dos usuarios distintos es muy improbable, como bien refleja la siguiente frase [12].

> "Just to give some perspective: in order to run out of addresses, each human currently living on the planet (±6 billions) has to generate 500 million of addresses for each single nano-second (10^{-9}s) during the entire age of the universe (15 billions of years)"

Estas direcciones identifican el destinatario de una transacción y, en principio, son anónimas ya que no almacenan información sobre el usuario. La generación de direcciones es sencilla y prácticamente instantánea, mediante cualquier software cliente de BTC. Para la realización de este TFG se ha usado el cliente "electrum", proyecto de código abierto, gratuito y ligero ya que no almacena toda la cadena de bloques, simplemente obtiene la información necesaria conectándose a la red de Bitcoin.

Ilustración 6. Creación de cartera a través de Electrum

La creación de un nuevo monedero es un proceso muy sencillo, en el que podemos elegir el tipo de cartera que queremos según se adecue más a nuestras necesidades. Las posibilidades para crearla son:

- Doble factor de autenticación (2FA): donde además de nuestra contraseña personal debemos introducir un número aleatorio de seis dígitos generado por la aplicación "Google Authenticator".
- Multi-firma: generar una dirección BTC, que a diferencia de la cartera estándar puede estar administradas por varias personas al mismo tiempo. La firma para autorizar una transacción no depende de un único usuario, sino que es posible configurar el número mínimo de firmas para generar una transacción. Por ejemplo, se puede crear una dirección multi-firma a partir de las claves de cinco usuarios, pero donde sólo sea necesaria tres de ellas para autorizar un movimiento.
- Importar una dirección Bitcoin que hayamos exportado con anterioridad en otro dispositivo.

A continuación, se genera una “semilla” compuesta por doce o trece palabras aleatorias, la cual debe recordarse y mantener en privado ya que nos permitirá recuperar la cartera en caso de que se produzca un fallo en el ordenador.

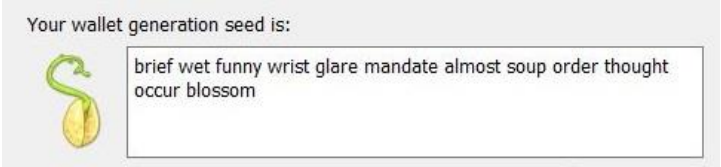
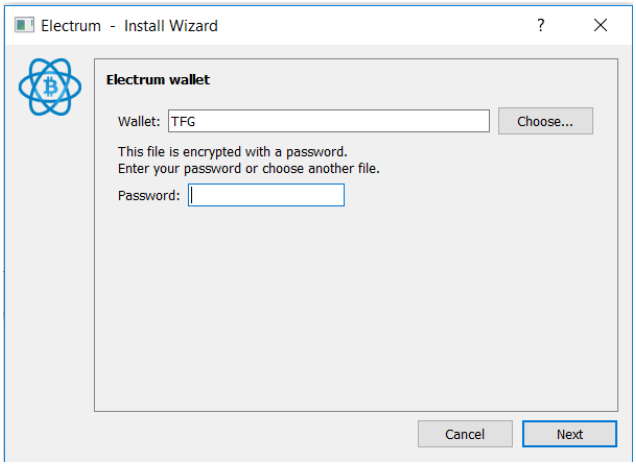


Ilustración 7. Semilla para recuperar cartera en caso de pérdida

La creación del monedero finaliza con el establecimiento de una clave privada necesaria para cifrar la semilla en el disco duro, lo cual nos permitirá identificarnos para acceder a la cartera y firmar transacciones.



Ilustración

En la actualidad, los tipos de monederos se pueden dividir en cinco grandes grupos: PC, móvil, online, dispositivo físico y carteras frías. La principal diferencia es la manera en que se almacenan las claves privadas: en el caso del PC y móvil se guardan en la propia memoria interna; en las carteras online el almacenamiento y distribución lo lleva a cabo una empresa externa de manera análoga a los bancos convencionales; los dispositivos físicos (monederos hardware) son dispositivos USB seguros e interactivos en los que los pagos se llevan a cabo mediante un sistema de autenticación por tokens; por último, las carteras frías o de papel son las claves impresas en papel, incluyendo en él la dirección BTC correspondiente y su representación en código QR que facilita la lectura al no tener que escribir la dirección manualmente.

A pesar del carácter básico de esta última técnica, es una manera efectiva y segura ya que, al no necesitar conexión a internet, evita las amenazas de hackers, *keyloggers* y otras amenazas en línea.

Dirección pública	Clave privada (WIF)	Código QR
1QL5THirpbgnysnu1zCHCYFnxTxCPrReu	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn	

Tabla 7. Estructura simple de una cartera de papel.

3.2.3 Transacciones

Las transacciones son la base del protocolo Bitcoin, ya que el objetivo del sistema es crear, propagar por la red, validar y registrar dichas operaciones en el blockchain. Son estructuras de datos codificadas y públicas.

Entradas (*Inputs*): para poder entender cómo funcionan las entradas, es indispensable saber qué son las salidas de transacciones no gastadas (*unspenttransaction output)* o UTXO.

Las UTXO son trozos indivisibles de BTC ligados a un propietario concreto, anotado en la cadena de bloques y reconocido por todos los participantes de la red. Cada vez que un usuario recibe una transferencia con bitcoins a su favor, ésta es registrada en el blockchain como una UTXO. De hecho, no existe el concepto de saldo en el protocolo Bitcoin, sino que es una nomenclatura usada por los monederos para hacer referencia al monto total de BTC que dispone un usuario en referencia a la cantidad de UTXO que le pertenecen. La transacción se crea a partir de una salida no gastada, la aplicación del monedero selecciona las UTXO del usuario de manera que compongan un valor igual o mayor que el de la salida [15].

Salidas (*Outputs*): registradas en el libro contable, contiene los campos donde se indican las direcciones a las cuales han de ser enviadas y el conjunto de BTC que se envía a cada destinatario. Se utiliza el sistema de unidad indivisible llamado Satoshi, que es equivalente al céntimo en el Euro (1 BTC = 10^8Satoshis). El valor de la salida debe ser

siempre igual o inferior al de entrada, nunca superior. Por ejemplo, en el caso de que dispongamos de un saldo de 7 BTC y queremos enviar 3 BTC a otro usuario, se crea de nuevo un *output* de 4 BTC con nuestra dirección, equivalente al cambio de la transacción [15].

Por último, para que la transacción se pueda llevar a cabo es necesario especificar la comisión que recibirán los mineros. Estas tasas de emisión sirven de aliciente para añadir la transacción en el siguiente bloque y así evitar abusos del sistema por des-incentivación el "spam" de micro transacciones. No son obligatorias, pudiendo ser las transacciones procesadas e incluidas en el siguiente bloque de igual manera, pero a medida que aumenta el número de usuarios se realizan más operaciones por minuto que pueden llegar a superar la capacidad de la red, necesitando más tiempo para procesarlas.

3.3 Monedero

Desde la creación de la criptografía de clave pública en la década de los 70, su aplicación en algoritmos de cifrado asimétrico impera en gran medida en los actuales sistemas de cifrado. El par de claves digitales son creadas y almacenadas por el propio usuario mediante el software del monedero y administradas por el mismo, sin relacionarse directamente con el protocolo Bitcoin o el blockchain. Sin embargo, se habilitan la confianza descentralizada y la comprobación de propiedad debido a las claves, donde cada transacción necesita una firma para ser incluida en la cadena. A la hora de realizar una transacción, la dirección de pago corresponde normalmente al *hash* de la clave pública, indicando quién es el beneficiario.

Clave pública**:**

Es generada a partir de la clave privada, mediante algoritmos de encriptación de curva elíptica. Es un proceso irreversible, lo que significa que es computacionalmente inviable obtener la clave privada a partir de la pública, operación conocida como "encontrando el algoritmo discreto" (búsqueda por fuerza bruta) [15]. Este es la razón por la que se puede compartir sin relevar la clave privada.

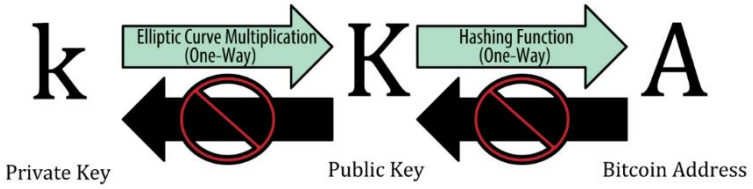


Ilustración 8. Creación de las direcciones de bitcoin [15]

Esta clave puede ser distribuida libremente y sirve para autenticar una firma. La generación de la clave empieza con una clave privada representada por un número aleatorio *k*, el cual se multiplica por el punto generador de la curva para obtener como resultado la clave pública *K* pertinente.

Direcciones BTC:

Una dirección de Bitcoin se representa mediante una cadena de dígitos y caracteres alfanuméricos, que puede ser publicada por cualquier usuario de la red que desee enviar una transferencia al dueño de la dirección. Deriva de una clave pública y normalmente empieza por 1 o 3 si se trata de una dirección multi firma. El número inicial las hace diferir en la seguridad de cada dirección: si empieza por 1 (*Ej. 122xMbJydf9NpHaCFzzCzma7CLT3h5mXQw)*, únicamente será necesaria la clave

privada del propietario para autorizar la transacción; mientras que si empieza por 3 corresponde a una dirección multi-firma, donde es necesario la validación de dos o más claves privadas ya que se necesita más de un participante para realizar le envío de bitcoins, lo que conlleva un incremento en la seguridad de la cuenta. Es común que este tipo de direcciones correspondan a empresas, donde disponen de una lista de posibilidades: multi-firma 10/10(se crea con 16 claves privadas y se necesitan las 16 para validad, alto nivel de seguridad), multi-firma 5/3, multi-firma 3/2… Actualmente existe páginas como "https://coinb.in/#wallet" donde se pueden hacer pruebas con direcciones multi-firma para visualizar el concepto.

Una dirección de Bitcoin no es equivalente a una clave pública; la mayoría de las veces son presentadas en "Base58Check", una codificación de 58 caracteres y un "*checksum*" que permite evitar los errores tipográficos del usuario al transcribir una dirección debido a la ambigüedad de algunos caracteres. El protocolo Bitcoin usa este tipo de codificación cada vez que el usuario debe introducir una dirección, el *hash* de un *scrip*t, una clave privada o una clave encriptada. Las direcciones se generan mediante doble *hash*: primero se aplica la función *hash* SHA-256 a K (clave pública), a la huella generada se le aplica de nuevo el *hash* RIPEMD160, por lo que obtenemos un número de 160 (20 bytes) [15].

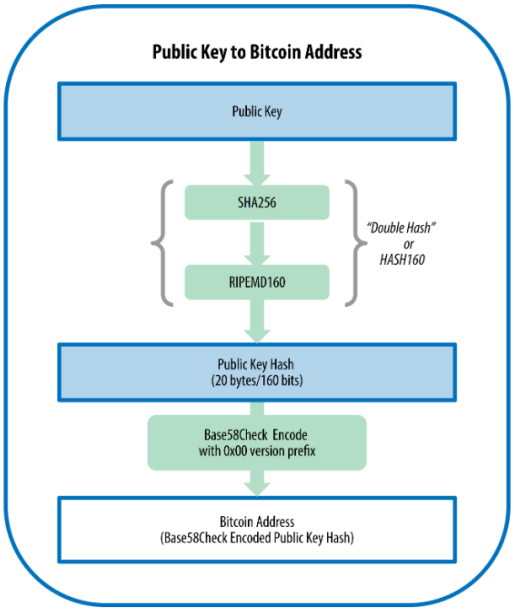


Ilustración 9. Conversión de una clave pública a una dirección de BTC

Clave privada**:**

La clave privada es un número de 256 bits generado de manera aleatoria. El valor de esta clave es primordial, ya que permite generar las firmas necesarias para gastar los fondos y se consigue el control del monedero, por lo que no debe ser compartida con nadie. Si se pierde esta clave, los BTC que queden dentro del monedero serán inaccesibles, esto se conoce comúnmente como "bitcoins destruidos", y no podrán recuperarse ya que no existe copia de seguridad debido a su carácter descentralizado.

El algoritmo matemático usado para la generación de la clave está basado en encontrar un número entre 1 y n-1 (siendo $n=1.158 \cdot 10^{77}$), un tanto menor que 2^{256} y coincidiendo con el orden de la curva elíptica usada en el protocolo Bitcoin. El algoritmo por el cual se llega a ese número puede ser diferente, siempre que no sea predecible ni repetible.

3.4 *Blockchain* o Cadena de bloques

Satoshi Nakamoto, nombre bajo el cual se esconde la persona o grupo responsable de la creación del protocolo Bitcoin y su software de referencia Bitcoin Core, define la cadena de bloques o *blockchain* como una base de datos compuesta por bloques relacionados entre sí que contienen todo el registro histórico de transacciones ordenado cronológicamente en el tiempo de manera pública, siendo accesible y compartida por todos los nodos que componen la red.

Esta red graba las transacciones en unidades de bloques, cada uno de los cuales incluye un identificador único propio y el del bloque que lo precede. El primer bloque o "bloque génesis", está definido como parte del protocolo. Un bloque válido incluye el *hash* del bloque previo, el hash de la transacción en el actual bloque, y una dirección de Bitcoin la cual corresponde a la dirección del primer minero capaz de resolver el acertijo matemático que acredita la veracidad del bloque. Este es el denominado proceso de minado, y por consecuencia, cuando se sella un bloque y se introduce en la cadena se denomina "minado de bloques". Este sistema permite aumentar la seguridad del sistema contra transacciones fraudulentas y evitar uno de los mayores problemas de las monedas digitales, el doble gasto o *double spending*, que consiste en hacer uso de las mismas monedas en diferentes operaciones. Cualquier nodo minero puede agregar un bloque válido a la cadena, simplemente debe publicarlo antes que los demás, obteniendo así la recompensa otorgada al primer minero en resolver la prueba de trabajo (*proof-of-work*). Si dos mineros resuelven el algoritmo de trabajo a la vez, con el mismo bloque predecesor, la cadena se bifurca en dos y se produce un *fork*.

Debido al tiempo de propagación que se produce desde que se sella un bloque hasta que llega a los nodos para que lo verifiquen, cada nodo extiende la cadena de bloques con el que le ha llegado primero. Estas incoherencias producidas por las bifurcaciones de la cadena se solucionan reconvirtiéndola a medida que se añaden más bloques a una de las bifurcaciones, siendo usualmente la subcadena más larga que conocen o a la primera de la que han oído hablar. Esto provoca que la ramificación que tenga menor apoyo debe ser eliminada, por lo que las transacciones incluidas en los bloques siguientes son ignoradas y los clientes pueden volver a realizarlas. Es por esto por lo que una transacción no se verificada hasta que la cadena añade seis bloques a continuación del que contiene la transferencia, es decir, seis confirmaciones.

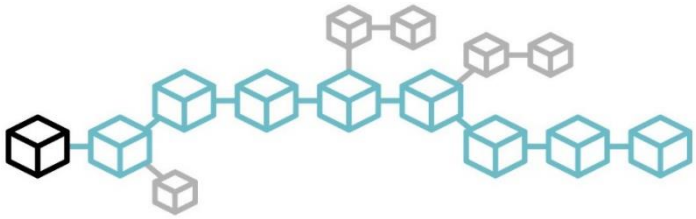


Ilustración 10. Bifurcación en la cadena de bloques [16]

El sellado de los bloques en el protocolo Bitcoin está programado para que se produzca cada 10 minutos, si este tiempo se ve reducido o aumentado, existe un campo de dificultad para la resolución del algoritmo de trabajo que se ajusta en medida que sea necesario para mantener este criterio [16].

Marker	Rank	Name	Status	Type	Links	Block	Supply	Ratio	Ratio Price	Price per Coin	1h	24h	7d
○	1	Bitcoin Cash (BCH)				478558 2017-08-01	21,000,000	1:1	Ƀ 0.07839469 $ 528.59	Ƀ 0.07839469 $ 528.59	0.2%	0.91%	-3.32%
○	2	Bitcoin Gold (BTG)				491407 2017-10-24	21,000,000	1:1	Ƀ 0.00292279 $ 19.68	Ƀ 0.00292279 $ 19.68	0.04%	-1.6%	1.33%
○	3	Bitcoin Diamond (BCD)				495866 2017-11-24	210,000,000	10:1	Ƀ 0.00181820 $ 12.24	Ƀ 0.00018182 $ 1.22	0.08%	0.43%	14.7%
○	4	Bitcoin Private (BTCP)				511346 2018-02-28	21,000,000	1:1	Ƀ 0.00062334 $ 4.20	Ƀ 0.00062334 $ 4.20	0.35%	5.17%	4.83%
○	5	Lightning Bitcoin (LBTC)				499999 2017-12-18	21,000,000	1:1	Ƀ 0.00136094 $ 9.16	Ƀ 0.00136094 $ 9.16	0.09%	0.86%	-6.04%
○	6	BitcoinX (BCX)				498888 2017-12-12	211 Billion	10k:1	Ƀ 0.00540000 $ 36.61	Ƀ 0.00000054 $ 0.00	-0.97%	4.18%	-22.96%
○	7	Nash (SBTC)				498888 2017-12-12	21,210,000	1:1	Ƀ 0.00070950 $ 4.78	Ƀ 0.00070950 $ 4.78	3.76%	-7.19%	65.69%
○	8	BitCore (BTX)				492820 2017-11-02	21,000,000	1:2	Ƀ 0.00008786 $ 0.59	Ƀ 0.00017573 $ 1.18	0.08%	-1.68%	-8.76%
○	9	CLAMs (CLAM)				300377 2014-05-12	16,557,684	N/A	Ƀ 0.00038488 $ 2.59	Ƀ 0.00038488 $ 2.59	-0.05%	-0.29%	20.2%
○	10	Bitcoin Interest (BCI)				505083 2018-01-20	21,000,000	1:1	Ƀ 0.00019035 $ 1.28	Ƀ 0.00019035 $ 1.28	1.34%	1.09%	4.41%
○	11	Bitcoin Atom (BCA)				505888 2018-01-24	21,000,000	1:1	Ƀ 0.00004499 $ 0.30	Ƀ 0.00004499 $ 0.30	0.14%	18.66%	0.51%
○	12	Segwit2X (B2X)				501451 2017-12-28	21,000,000	1:1	Ƀ 0.00003049 $ 0.21	Ƀ 0.00003049 $ 0.21	-0.28%	-0.58%	-23.11%

Ilustración 11. Recopilación algunas bifurcaciones de bitcoin. [66]

La particularidad del algoritmo de prueba de trabajo es que es muy complejo encontrar dos entradas diferentes que produzcan el mismo *hash*. Por tanto, la única manera de encontrar una huella digital determinada es probar con entradas aleatoriamente. A continuación, se muestra el *hash* de la frase "Universidad Carlos III" con una herramienta on-line (https://hash.online-convert.com/es/generador-sha256).

Texto	Hash (SHA256)
Universidad Carlos III	4da5d9ac82f3f0c51648eeef0a4d849314be363d21c403d255560fb79f5cd1ce
Universidad Carlos III1	68615e16f757b9aad2755fbbdf57a6895218ff8ef4253663c978ca4c8b39807e
Universidad Carlos III2	95f68d4ce301f8eb20a0f5619d5bfcf177283b7115af172936e4c2b980fce112
Universidad Carlos III3	5abcad17b0770dd7764807176df571a3487a23c878e86ac52ec2d7f67aa1f6f7
Universidad Carlos III4	285ef6c6febf3c762367a9b5c744529d62e15fc73bd9d87b98c6c5b71a854e03

Tabla 8. Ejemplo de hashes SHA256

Como se puede apreciar, la mínima modificación en el texto, ya sea una mayúscula, un signo de puntuación o un espacio, genera un *hash* resultante completamente distinto, quedando así demostrado la imposibilidad de elegir un *hash* determinado a partir de la entrada.

El algoritmo de prueba de trabajo se basa en esta propiedad. El número concatenado al final de cada texto se llama *nonce* y se utiliza para validar la salida de una función criptográfica. Un ejemplo de prueba de trabajo podría ser encontrar una salida cuyo *hash* hexadecimal comience por 0. Particularizando a nuestro caso no es complicado, ya que al intento número 15 ("Universidad Carlos III15") genera la siguiente huella digital: "00be470bc6d3e8b4b8490a6706fd4041ffad3fea8688a9d5ac8eda26a6874240".

Si cambiamos el objetivo y queremos obtener un hash hexadecimal que empiece por 4 ceros la dificultad computacional y el tiempo invertido aumentan considerablemente. Esta autorregulación de dificultad por el protocolo Bitcoin permite que se minen los bloques aproximadamente cada 10 minutos; a medida que los mineros invierten más dinero en poder computacional, la dificultad del minado aumenta consecuentemente.

TAMAÑO	CAMPO	DESCRIPCIÓN
4 bytes	Versión	Versión que indica los protocolo establecidos
32 bytes	Hash del anterior bloque	Referencia al hash padre
32 bytes	Árbol de Merkle	Hash de la raíz del árbol
4 bytes	Hora	Tiempo de creación del bloque (seg. Desde Unix Epoch)
4 bytes	Dificultad	Dificultad del algoritmo de "proof of work"
4 bytes	Nonce	Identificador usado en el "proof of work"

Tabla 9. Estructura de la cabecera de un bloque

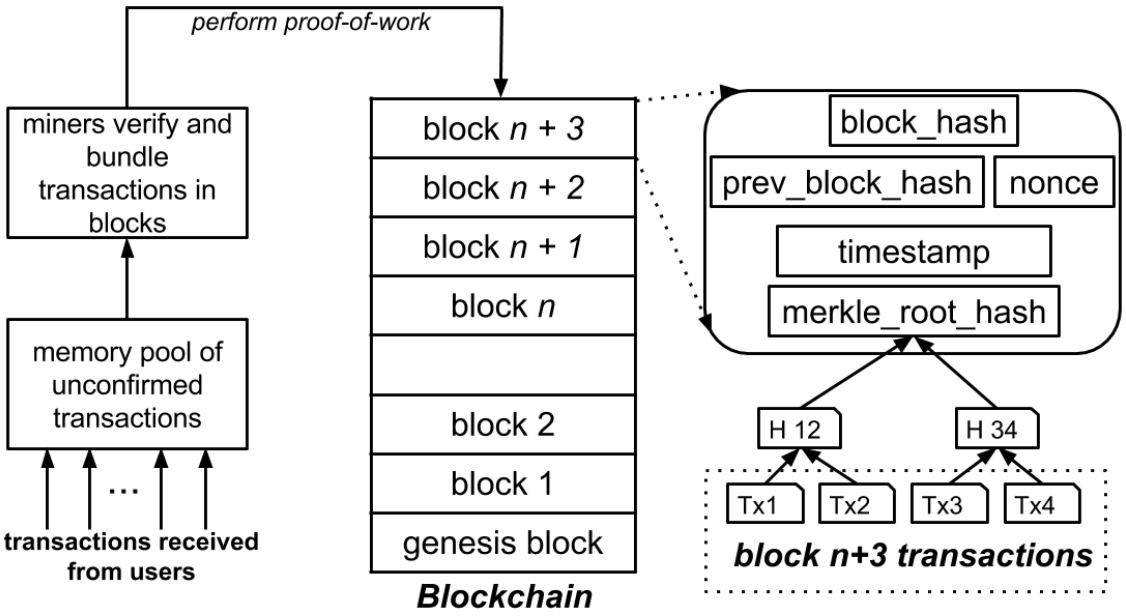


Ilustración 12. Creación y adición de bloques en el blockchain

Cada bloque dentro de la cadena se identifica por un *hash* en la cabecera, generado por el algoritmo SHA-256. Dicho *hash* está incluido en la cabecera del bloque y le identifica de manera unívoca.

Debido al gran tamaño de la cadena, el protocolo Bitcoin contiene un resumen del registro histórico de todas las transacciones mediante el "árbol de Merkle" o árbol binario. Esta estructura jerárquica se usa para verificar de modo eficiente la totalidad de un gran volumen de datos, de modo que los nodos que no tengan descargada la cadena de bloques completa sean capaces de verificar si una transacción ha sido incluida en el bloque [15].


```
block 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
{
    "hash" : "000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
    "confirmations" : 308321,
    "size" : 285,
    "height" : 0,
    "version" : 1,
    "merkleroot" : "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
    "tx" : [
        "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"
    ],
    "time" : 1231006505,
    "nonce" : 2083236893,
    "bits" : "1d00ffff",
    "difficulty" : 1.00000000,
    "nextblockhash" : "00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048"
}
```


Ilustración 13. Ejemplo de cabecera de un bloque

3.4.1 Nodos de la red

La principal característica del protocolo se basa en la arquitectura de red P2P sobre la que trabaja. Los nodos que conforman la red se conectan entre ellos sin necesitar un servidor central ni una estructura organizada, por lo que proporcionan y consumen servicios al mismo tiempo, derivando en una red descentralizada, sólida y pública para cualquier usuario que participe de manera activa o no.

Dependiendo de las características de cada nodo desempeña unas funcionalidades u otras. La red está dividida en cuatro grandes grupos: "Wallet", "Miner", "Full Node" y "Network RoutingNode". Los nodos son necesarios para llevar a cabo las transacciones en la redy hay funcionalidades básicas que comparten todos ellos, como el enrutamiento de la red, la interconexión con los demás nodos de la red o la validación y propagación de transacciones y bloques. Los nodos completos o *full nodes* disponen de una copia completa y actualizada de la cadena de bloques que les permite verificar cualquier transacción de manera autónoma. Para disponer de una copia completa de la cadena se necesitan actualmente más de 180 Gb de almacenamiento, por lo que existen nodos de peso ligero como monederos que no necesitan la copia completa, si no que se

basan en conexiones con un nodo de confianza; se denominan nodos SPV ya que tienen la funcionalidad de *SimplifiedPaymentVerification [15].*

3.5 Ataques cibernéticos

Bitcoin es la criptomoneda más popular y un referente para el resto en cuanto al mercado de inversión de capitales. Debido a que se trata a un modelo descentralizado en un entorno incontrolable, ha generado un ambiente fraudulento donde hackers y ladrones encuentran una vía para delinquir. Además del doble gasto (teóricamente, imposible en Bitcoin), también cabe destacar los ataques que afectan a la billetera del cliente, ataques de red (como DDoS, sybil y eclipse) y ataques de minería. A continuación, se describirán algunos de los más conocidos.

El "*doublé spending"* o doble gasto es un problema potencial exclusivo de las monedas digitales porque la información digital se puede reproducir con cierta facilidad. Las monedas físicas no tienen dicho problema ya que no se pueden replicar fácilmente, y las partes involucradas en la transacción pueden comprobar de inmediato la veracidad de la moneda física. Sin embargo, con la moneda digital existe el riesgo de que el titular pueda hacer una copia del "*token"* digital y enviarla al destinatario manteniendo la parte original. Desde la creación de Bitcoin este ha sido uno de los mayores inconvenientes a tratar, ya que se trata de una moneda sin una entidad central que verifique el origen de los fondos. En Bitcoin, la red de mineros se encarga de verificar y procesar todas las transacciones, de esta manera se aseguran que sólo las monedas no gastadas que se especifican en las salidas de las transacciones anteriores se pueden usar como entrada. Es regla se aplica dinámicamente en tiempo de ejecución para proteger la red contra el posible doble gasto. El "*time-stamping"* distribuido y la PoW ("*Proof-of-Work"*) basado en un protocolo de consenso para ordenar de manera ordenada las transacciones en el blockchain. Por tanto, si un minero recibe dos transacciones con la misma entrada, podrá identificar que ambas transacciones están tratando de usar las mismas monedas durante la propagación de la transacción, por lo que procesa una y rechaza otra.

Una forma de doble gasto llamada "*finney attack" [25],* donde un cliente deshonesto (X1) pre-mina un bloque que contiene la transacción (Tx_1), y luego crea una transacción (Tx_2), usando los mismos bitcoins para el vendedor (X_2). El bloque minado no está registrado en la red, y cliente X espera hasta que la transacción (Tx_2) es aceptada por el vendedor. Por otro lado, X_2 sólo acepta (Tx_2) cuando recibe una confirmación de los mineros indicando que (Tx_2) es válida y se ha incluido en un bloque existente. Una vez X1 recibe el producto del vendedor, libera el bloque pre-minado en la red, por lo tanto, crea un "*fork"* (bifurcación de la cadena de bloques) de la misma longitud que la bifurcación existente. Ahora, si el siguiente bloque minado extiende la cadena forzada

por el atacante, todos los mineros construirán a continuación del bloque introducido por X1 e ignorando la cadena original; lo que significa que la transacción introducida de manera ilegal queda validada, por lo que el cliente recibirá de vuelta las monedas a través de una transacción que se realiza a sí mismo, pero quedando invalidada (Tx_2), debido a que la transacción queda en la cadena que ha sido ignorada por los mineros. Para evitar esto, el vendedor simplemente debe esperar a una múltiple confirmación antes de enviar el producto al cliente, es decir, que se sellen seis bloques posteriores al que incluye la transacción, ya que se considera computacionalmente imposible revertir dicha cadena.

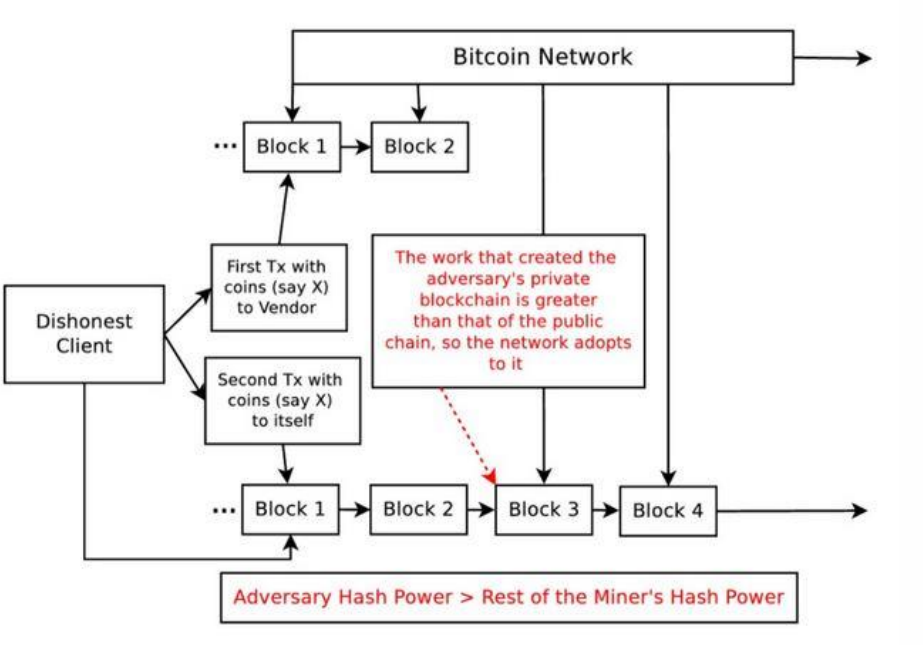


Ilustración 14. Doble gasto [24]

Para evitar el ataque "*Finney*", el vendedor debería esperar la múltiple confirmación antes de enviar el producto al cliente. La espera de la múltiple confirmación únicamente dificultará el doble gasto al atacante, pero la posibilidad aún permanece. Una versión avanzada del ataque de Finney es el llamado ataque de fuerza bruta [26] donde un atacante con muchos recursos se hace con el control de n nodos en la red, y esos nodos trabajan colectivamente minando un esquema privado con el objetivo de llevar a cabo el doble gasto. Un atacante introduce una doble transacción en un bloque como en el caso anterior, mientras continúa trabajando en la extensión del blockchain privado (*B´fork)* [24]. En el caso que el vendedor espero *X* confirmaciones antes de aceptar la transacción, y enviar el producto al cliente. Después, el atacante es capaz de minar los *X* número de bloques por delante y liberar estos bloques en la red; al ser la cadena falsa

de mayor longitud que *B Fork,* se extenderá el blockchain B por todos los nodos mineros de la red. Esto provocaría los mismos efectos que los descritos anteriormente por el ataque de Finney, lo que se traduce en un ataque exitoso de doble gasto

Por otro lado, existen otros ataques que atacan las vulnerabilidades en la implementación y diseño del protocolo Bitcoin y la comunicación entre pares. El ataque más conocido en el denominado *"DistributedDenial-of-Service"* (DDoS), cuyo objetivo son las casas de intercambio de criptomonedas, las piscinas de minado, monederos, y otros servicios financieros en Bitcoin. Debido a la naturaleza distribuida de la red de Bitcoin y su protocolo de consenso, la ejecución de un ataque DoS prácticamente no provoca un efecto negativo en el funcionamiento de la red, por lo que los atacantes tienen que lanzar un DDoS potente para alterar las funcionalidades de la red. A diferencia del ataque DoS, en el que un solo atacante lleva a cabo el ataque, en DDoS, varios atacantes lanzan el ataque al mismo tiempo. Los ataques de DDoS no son costosos computacionalmente, pero son bastante perjudiciales, ya que pueden llegar a colapsar un sistema, dejándolo así inutilizable. Los mineros maliciosos pueden realizar un DDoS (al tener acceso a una red distribuida) con objetivo los mineros honestos, reduciendo el número mineros operativos y, por ende, aumentando la potencia de hash del grupo de mineros maliciosos. En este tipo de ataques, el adversario agota los recursos de la red para interrumpir su acceso a los usuarios honestos de la red. En un ejemplo práctico, un el atacante congestionaría al minero con solicitudes (como transacciones falsas) provenientes de una gran cantidad de nodos malignos controlados por el atacante. Después de un tiempo, el minero es probable que comience a descartar todas las solicitudes entrantes incluyendo las de los clientes honestos.

Los conocidos ***"Malleabilityattacks"*** [30]. Mediante el uso de este tipo de ataque, el adversario obstruye la cola de transacciones. Esta cola consta de todas las transacciones pendientes que están a punto de ser atendidas por la red. Mientras tanto, un adversario realiza transacciones falsas con alta prioridad que representa al usuario que paga las tasas más altas por transacción. Cuando los mineros intentan verificar estas transacciones, encuentran que esta es la transacción falsa, pero en ese momento ya han dedicado una considerable cantidad de tiempo a verificar estas transacciones falsas. Este ataque desperdicia el tiempo y recursos de los mineros y de la red.

3.6 Riesgos y oportunidades en niveles macro, meso y micro

Las criptomonedas ponen en riesgo negocios y sociedades en muchos niveles de la sociedad. A continuación, se analizará el marco establecido en la sociedad, más específicamente en la economía evolutiva a niveles de micro, meso y macro. Donde micro se centra en acciones de un usuario individual, el nivel macro regional, estatal, nacional... (un sistema de nivel agregado) y el nivel meso que hace referencia a un nivel intermedio como instituciones y organizaciones.

Nivel Micro: En el *paper* escrito por Brito y Castillo [31], se enfatiza en el hecho de que las criptomonedas no son un refugio seguro para el ahorro personal debido al "riesgo de eliminación accidental o extravío". La pérdida de criptomonedas es casi imposible de recuperar, como sucedió a los usuarios que perdieron 650.000 Bitcoins debido al cierre del *exchange* "Mt. Gox" [33]. Esto es una realidad que ha de tenerse en cuenta en cualquier evaluación ética de las criptomonedas. No es raro que los usuarios afectados por el robo de criptomonedas no se refieran a usuarios con alta solvencia, ya que el aumento de valor y la popularidad de estas criptomonedas se ha convertido en una opción de inversión para usuarios sin grandes conocimientos financieros que apuestan por los activos en criptomonedas como medio de inversión bursátil con rentabilidad a corto plazo debido a la gran variación en su valor.

Nivel Meso: El uso de criptomonedas por parte de, entre otros, millones de trabajadores inmigrantes representa un riesgo existencial para los proveedores de servicios como "WesterUnion", que anteriormente cobraba hasta un 17% en tarifas de transferencia de dinero. Este ejemplo resalta el potencial disruptivo de las criptomonedas para el sector financiero. La tecnología Blockchain ofrece intercambios casi instantáneos para transacciones en todo el mundo a un costo mínimo. Sin embargo, debido a su enorme volatilidad en momentos de crisis, las criptomonedas aún no pueden cumplir adecuadamente varias de las funciones importantes de las monedas estándar, incluido, sobre todo, el almacenamiento de valor.

Nivel Macro: Cada vez un número cada vez mayor de individuos, instituciones y comunidades están optando por abandonar las monedas tradicionales para escapar del control gubernamental o bancarios considerados corruptos o ilegítimos, algunos con la expectativa del uso de criptomonedas para revolucionar el sistema económico [35]. Debido a la falta de mecanismos gobierno y marcos regulatorios, los usuarios de criptomonedas son susceptibles a la enorme volatilidad del intercambio del valor de las criptomonedas. Algunos estudios especulativos ofrecen una evaluación más medida, donde se sugiere que si se regula de forma inteligente, las criptomonedas podrían contribuir a una disminución general en la volatilidad de los activos financieros ofreciendo oportunidades de inversión contra cíclica (de manera similar al oro) y otros activos "naturalmente escasos" [36].

4. PRIVACIDAD Y ANONIMATO EN BITCOIN

El objetivo de mantener el anonimato es doble, por un lado, es deseable que una dirección de Bitcoin no vincule a una persona, un mail, una IP de usuario... por otro lado, que las direcciones de Bitcoin no puedan ser relacionadas unas con otras.

Los problemas de seguridad en Bitcoin están estrechamente relacionados con la privacidad de la transacción y el anonimato del usuario. En Bitcoin en este momento, los usuarios no son realmente anónimos. El monitoreo sistemático de la red entre pares no encriptada de Bitcoin y el análisis de la cadena de bloques pública pueden revelar mucha información, como quién usa Bitcoin y con qué fines. Los usuarios puede que no quieran que todo el mundo sepa en qué se gastan el dinero, cuánto tienen o cuánto ganan. Del mismo modo, las empresas pueden no querer filtrar detalles de las transacciones a su competencia.

El sistema bancario tradicional logra un nivel de privacidad al limitar el acceso a la información de las transacciones a las entidades involucradas y a la parte verificadora. Mientras en Bitcoin, el blockchain público revela todos los datos de las transacciones de cualquier usuario conectado a la red. Sin embargo, la privacidad aún puede ser mantenida hasta cierto nivel al romper el flujo de información en algún lugar de la cadena de procesamiento de transacciones de Bitcoin; esto se logra manteniendo las claves públicas anónimas, es decir, el público puede ver que alguien está enviando una cantidad a alguien, sin embargo, sin información vinculante de la transacción con nadie. Para mejorar aún más la privacidad del usuario, se recomienda utilizar un nuevo par de claves para cada transacción para evitar que sea vinculada a un usuario en particular. Sin embargo, la vinculación aún es posible en transacciones de múltiples entradas, que necesariamente revelan que sus entradas pertenecen al mismo usuario. Además, si la identidad del propietario de la clave se revela, existe el riesgo de que la vinculación podría revelar otras transacciones que pertenecen al mismo usuario. En particular, Bitcoin ofrece una desvinculación parcial (es decir, pseudónimo), y por lo tanto es posible vincular una cantidad de transacciones a un usuario en particular rastrando el flujo de dinero a través de un análisis robusto de la cadena de bloques. La tecnología Bitcoin se mantiene cuando se trata de la privacidad, pero la única privacidad que existe en Bitcoin proviene de direcciones pseudónimas (claves públicas o sus hashes) que son frágiles y fácilmente comprometidos a través de diferentes técnicas como la reutilización de direcciones de Bitcoin, análisis de “contaminación”, seguimiento de pagos a través de métodos de análisis del blockchain, nodos de monitoreo de direcciones IP, web-spidering… Una vez que se rompe, esta privacidad es difícil y algunas veces costoso recuperar. Bitcoin no tiene ningún directorio para mantener el registro u otra información relacionada con la transacción, sin embargo, un adversario puede

asociar los datos fuera de línea, como correos electrónicos y envío de direcciones con la información en línea, y puede obtener la información privada sobre los pares.

El anonimato completo en Bitcoin es un tema complicado. Para imponer el anonimato en las transacciones, Bitcoin permite a los usuarios generar múltiples direcciones de BTC, por lo tanto, el adversario que intenta desanonimizar necesita construir un mapeo de “uno a muchos” entre el usuario y sus direcciones asociadas, En particular, los usuarios de Bitcoin pueden estar vinculados a un conjunto de direcciones públicas mediante el uso de un procedimiento de análisis detallado del blockchain. Una manera de encontrar una vinculación en el nivel de protocolo de Bitcoin es asumir que todas las entradas en una transacción son generadas por el mismo usuario, ya que en la práctica rara vez varios usuarios contribuyen en una transacción única y colaborativa.

Bitcoin no proporciona un verdadero anonimato: las transacciones implican direcciones seudónimas, es decir, las transacciones de un usuario a menudo se pueden vincular fácilmente entre sí. Además, si alguna de esas transacciones está vinculada a la identidad del usuario, todas las demás pueden ser expuestas. Esto ha llevado a un aumento de servicios de mezcla *(“mixers”) cuyo* objetivo es recibir las monedas de un usuario (cliente del servicio) y cambiarlas aleatoriamente por monedas de otros usuarios para ofuscar la trazabilidad de las mismas, aunque estas no cuentan con protección contra el robo por parte del propio servicio, es decir, es un servicio basado en la confianza del cliente. La comunidad de Bitcoin es consciente de este problema, por lo constantemente se busca un mayor nivel de anonimato. Estas propuestas existentes pueden dividirse en dos grupos principales, primero las que proporcionan un gran anonimato, sin embargo, requieren criptografía avanzada y modificaciones sustanciales en el protocolo Bitcoin, como “Zerocoin”, o incluso el uso de otra criptomoneda creada con el objetivo de palear estas carencias de anonimato que tiene Bitcoin, como “Zercash”. En segundo lugar, hay propuestas como “CoinJoin” o “CoinSwap”, servicios de mezcla de BTC que son compatibles con el protocolo Bitcoin, pero tienen complicaciones en la práctica y proporcionan un menor nivel de anonimato.

4.1 Mixers

Debido al hecho de que todas las transacciones se almacenan públicamente en el blockchain, el anonimato de un emisor se basa en que no exista vínculo alguno entre el pseudónimo y su verdadera identidad. Por lo general, los usuarios deben proporcionar información personal para poder comprar bitcoins, por lo que desde un primer momento se almacena la información personal del usuario en la web donde se adquieren los bitcoins.

A continuación, se muestra el procedimiento paso a paso necesario para poder abrir una cuenta en el *exchange* "CoinBase", uno de las casas de intercambio de bitcoin más populares.

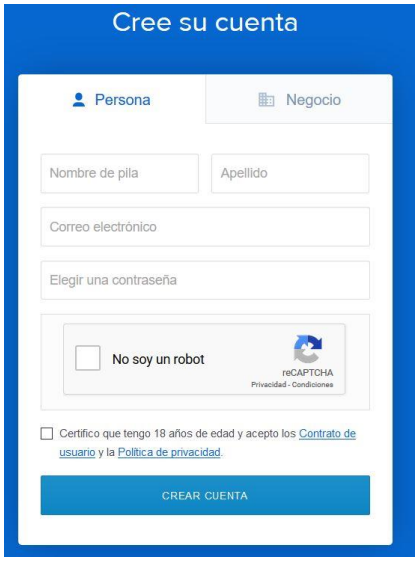


Ilustración 17. Registro Coinbase, paso 1.

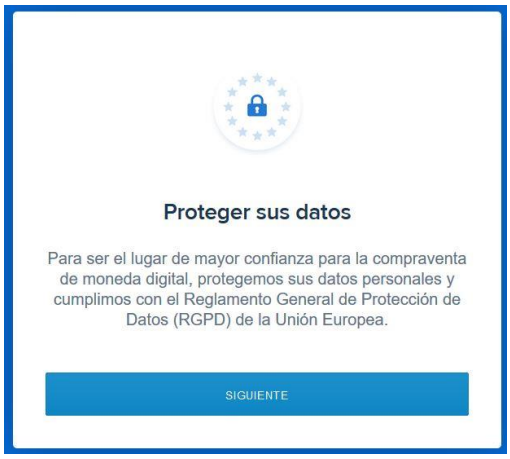


Ilustración 16. Registro Coinbase, paso 2.

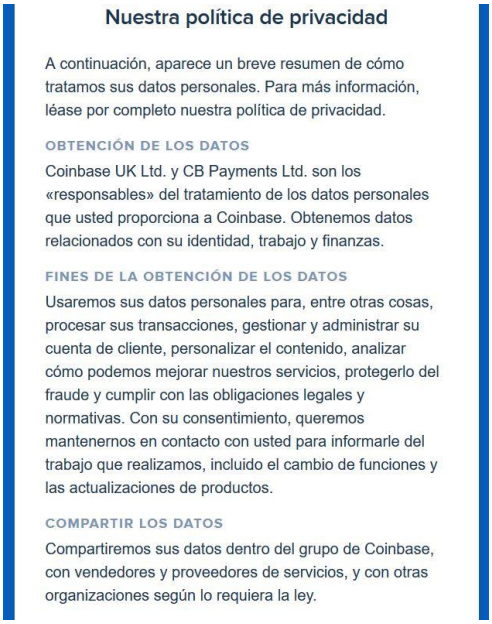


Ilustración 15. Registro Coinbase, paso 3.

Las imágenes anteriores corresponden a los primeros 3 pasos en un nuevo registro en la casa de intercambio. Requiere información sobre el tipo de usuario que va a hacer uso de la cuenta, tanto si es un particular como si se trata de un negocio. Una vez proporcionada tu identidad te hacen saber las políticas de privacidad a las que está sujeta al Reglamento General de Protección de Datos(RGPD).

"El RGPD -EDL 2016/48900- establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos. Se considera "dato personal" toda información sobre una persona física identificada o identificable (el interesado) y como "tratamiento" cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no."

Si se realiza una lectura detenida a la política de privacidad [figura 15], se puede leer lo siguiente: *"COMPARTIR LOS DATOS: Compartiremos sus datos dentro del grupo de Coinbase, con vendedores y proveedores de servicios, y con otras organizaciones según lo requiera la ley"*

Ilustración 18. Registro Coinbase, paso 4.

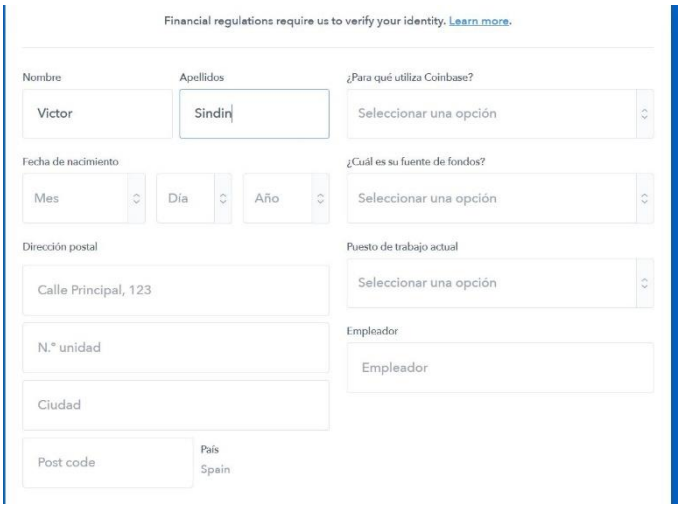


Ilustración 19. Registro Coinbase, paso 5.

En los siguientes pasos se piden una detallada información personal, incluyendo desde el número de teléfono hasta la dirección exacta y trabajo actual del usuario.

Recientemente, Coinbase ha aumentado sus requisitos de identidad.

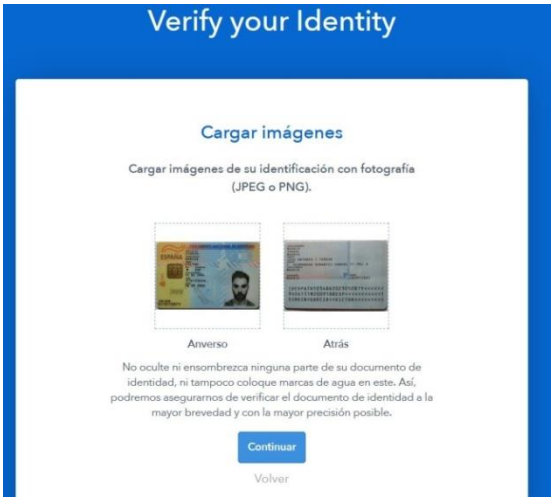


Ilustración 19. Registro Coinbase, paso 6.

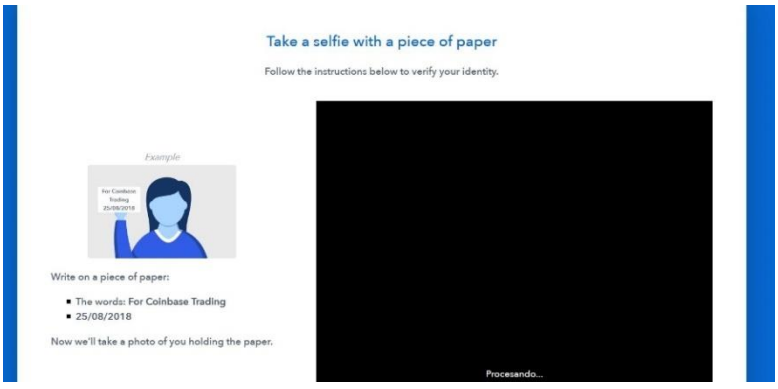
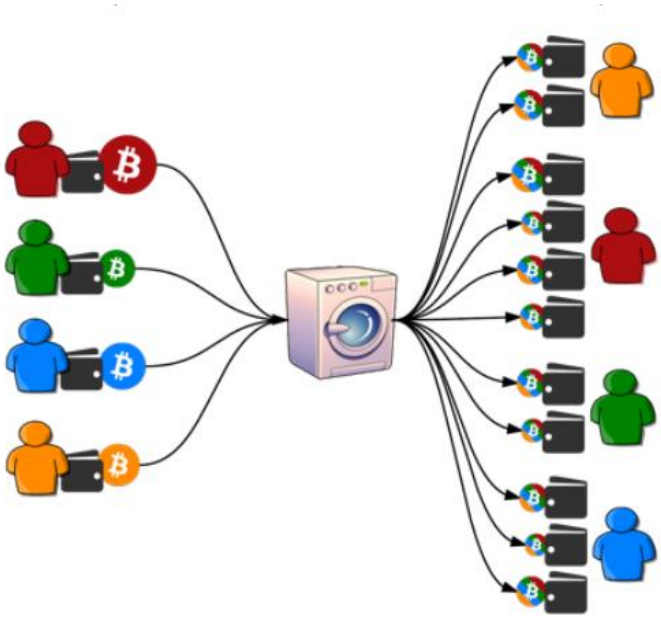


Ilustración 20. Registro Coinbase, paso 7.

Por último, para poder depositar o retirar monedas es necesario tanto un escaneo del documento de identidad, como un "selfie" sujetando un papel que tenga escrito "*For Coinbase Trading*". Toda esta información aportada para poder realizar una compra de criptomoneda queda almacenada y manipulada libremente por el *exchange* para usos descritos anteriormente en la política de privacidad; esto hace que la identidad del usuario esté completamente vinculada a su cartera. Para desvincular los bitcoins de la verdadera identidad de una persona, podrían intentar usar un servicio de mezcla para transferir bitcoins a una nueva dirección anónima. Las mezclas de Bitcoin son servicios que pretenden aumentar el anonimato al mezclar las monedas de múltiples usuarios, lo que hace más difícil encontrar una relación entre las transacciones de entrada y la salida aumentando el nivel de anonimato. "*Anonymity means, that an entity inside a set of other entities (the anonymity set) is not identificable"* [51].

Las transacciones en una cadena de bloques como Bitcoin son públicas y mantienen un vínculo entre ellas, lo cual permite mediante técnicas como el análisis grafo, el cual permite aprovecharse de los enlaces que hay entre entradas y salidas pertenecientes a transacciones en el blockchain (el emisor de la y el receptor). Es necesario seguir el flujo de fondos de la dirección origen a la dirección de pago, por lo que existe la posibilidad de observar el rastro de las monedas, por el contrario, no es trivial adjudicar de manera directa una dirección Bitcoin a un usuario determinado.

Para ocultar la identidad del usuario existen técnicas de ofuscación de datos, como la proporcionada por los *mixers*, donde los usuarios de Bitcoin pueden dificultar el rastreo de sus transacciones haciendo uso de dicha técnica, la cual combina los fondos de un gran número de usuarios, mezcla y envía de vuelta a diferentes direcciones, en diversos instantes de tiempos y en cantidades fraccionadas más pequeñas.



Estos servicios de terceros se apropian de los bitcoins de todos los usuarios que participan en la mezcla durante un tiempo, periodo en el que se combinan las monedas entre sí, antes de enviarlas de nuevo al usuario que ha contratado el servicio.

Los servicios de mezcla generalmente cobran un porcentaje de los fondos mezclados, aproximadamente entre 3-5% de la cantidad total que se desea mezclar, En la implementación común el *mixer* proporciona una "dirección de mezcla" que recibe monedas de múltiples clientes y las envía al azar a una nueva dirección para cada cliente tras miles de transacciones. Como medida de precaución, se recomienda acceder a través de Tor para ocultar la dirección IP en el caso de que el servicio almacene registro de actividad de los usuarios [52]. Estos servicios son a menudo utilizados por clientes malintencionados, piratas informáticos, estafadores y criminales que usan *ransomware* y amenazan con "Distributed Denial of Service" (DDoS) como forma de extorsión a cambio de bitcoins, sin embargo, también los utilizan personas que no estás involucradas en actividades ilícitas o delictivas, pero desean preservar la privacidad de sus transacciones de Bitcoin. Por lo tanto, el uso de dicho servicio no implica necesariamente que el usuario haya participado en actividades delictivas o ilícitas, a pesar de ello, los usuarios de los *mixers* mezclarán sus transacciones con las que se dedican a actividades ilícitas, contaminando así las transacciones. Es importante destacar que la eficacia de estos servicios varía de unos a otros, de hecho, según el análisis de los servicios de mezclado realizado por Malter Möser [41] hay algunos servicios en los que el análisis de contaminación era inmediato, suficiente para vincular la entrada y la salida; quedando demostrado que no todos servicios de mezcla ofrecen los mismos resultados.

Para que este tipo de mezcla sea efectiva, el mezclador necesita muchos usuarios con gran cantidad de BTC´s para poder realizar una mezcla en una cartera común de forma eficaz; cuanto más tiempo pasen las criptomonedas dentro del servicio en cuestión, más eficaz será debido al aumento de transacciones llevadas a cabo hasta que las monedas son enviadas de vuelta. Por otro lado, el uso de este tipo de servicios conlleva un riesgo asociado; el mezclador podría quedarse con las monedas, podría cerrar o incluso ser hackeado en ese mismo periodo. Además, el mezclador también sabe a dónde se envían las monedas de casa usuario, por lo que, si mantiene un registro y alguien accede a este, el efecto de la mezcla quedaría anulada. Estos servicios son casi siempre anónimos, por lo que el usuario no tiene ningún recurso si el mezclador realiza cualquier acción que comprometa la mezcla, y, por ende, el anonimato del cliente.

4.2 CoinJoin

El principal inconveniente de los servicios de mezcla es la necesidad de confiar en terceras partes y que no guarden registro de la actividad, siendo esto último legalmente imposible debido a la ley de conservación (05/2007) de 18 de octubre *"con el fin de posibilitar que dispongan de ellos los agentes facultados"* [69], por lo que la única posibilidad sería la configuración de VPN, el uso de la red Tor o incluso el acceso a un *mixer* albergado en la *deep web.*

CoinJoin es una técnica de mezcla de criptomonedas que intenta eliminar el requisito de confiar en terceros; usa la propiedad de las transferencias que hace referencia a que una única transacción puede tener múltiples entradas y múltiples salidas. Por ejemplo, si Alice y Bob quieren enviar una transacción a Charly y a Darius respectivamente, entonces pueden combinar ambos envíos en una sola transacción, de manera que tendrá dos entradas (Alice y Bob), y dos salidas (Charly y Darius). El orden de las entradas y salidas se distribuye de forma aleatoria, por lo que no es posible diferencias al receptor de la transacción; se puede interpretar de igual forma tanto que Charles recibe un bitcoin de Alice o Bob, o que tanto Alice como Bob envían medio bitcoin a Charles, de esta forma, cuantas más personas participen en este proceso, mayor será la incertidumbre del emisor y del receptor.

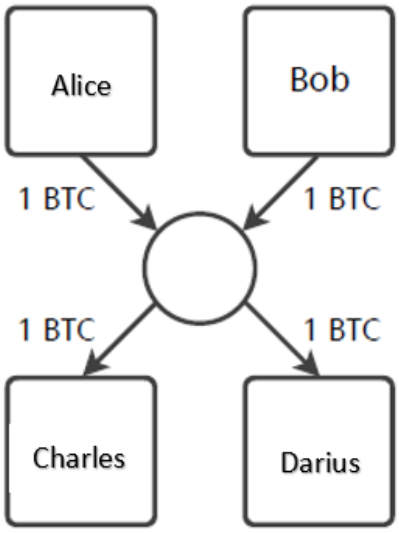


Ilustración 21. Transacción CoinJoin. [52]

No se necesita un tercero de confianza para retener las monedas según lo requerido cuando usamos un *mixer*, pero todas las partes involucradas en una transacción de CoinJoin deben comunicarse entre sí para firmas la transacción conjunta. Esta coordinación es difícil por varias razones. Primero, en un momento dado, es posible que no haya suficientes personas que quieran participar en una transacción conjunta. En segundo lugar, los participantes en este tipo de transacciones pueden saber quién está participando y tienen la capacidad de deshacer la mezcla. Es posible el uso de un servicio de terceros para coordinar las transacciones conjuntas, pero esto lleva de nuevo al segundo caso, la tercera parte implicada conoce el patrón de mezclado y podría deshacerlo.

CoinShuffle es una técnica propuesta para permitir las transacciones descentralizadas CoinJoin donde todas las partes que participan puedan crear la transacción sin un tercero de confianza y en la que ninguna de las partes tiene conocimiento de cómo descomprimir la transacción conjunta, además de conocer sus propias direcciones de entrada y salida. Algunas debilidades de CoinShuffle son, como CoinJoin, la posibilidad de que no haya suficientes usuarios participando para que la mezcla sea efectiva, y hay una mayor sobrecarga de comunicación [54]. De esta manera, si tres usuarios (X, Y, Z) que desean iniciar una transacción coinjoin, X debe usar la clave pública de Z para encriptar el destino de X, y enviará este mensaje a Y, el cual usará de nuevo la clave pública de Z para encriptar el destino de Y y enviará ambos mensajes a Z. Z ahora puede descifrar ambos mensajes y conocer los tres destinos. Z puede configurar la transacción y firmarla, luego la pasará a X e Y. Todas las partes solo firmarán si la transacción contiene los destinos correctos y ninguna parte puede desvincular las transacciones de las otras partes.

5. BITCOIN CORE

5.1 Cliente Bitcoin

El cliente del protocolo Bitcoin se llama *Bitcoin Core,* es un software de código libre que permite al usuario formar parte de la red como nodo de Bitcoin mediante la verificación de transacciones. Para realizar la sincronización con el sistema es necesaria una copia completa de la cadena de bloques, en la actualidad aproximadamente 180 Gb. Esta herramienta provee al usuario de una cartera propia, la cual verifica completamente los pagos.

Las carteras contienen las claves privadas que permiten firmar transacciones, con una estructura similar a la de una base de datos. Es importante aclarar que la cartera de bitcoin contiene claves, no monedas. Cada usuario posee una cartera que contiene las claves necesarias para realizar transacciones, un mismo monedero a su vez ofrece la posibilidad de generar tantas direcciones como se desee, práctica altamente recomendable para aumentar el anonimato. Las carteras son en esencia llaveros que almacenan de manera estructurada pares de claves privadas/públicas. Los usuarios firman transacciones con las claves, demostrando de esa forma que son dueños de las salidas de transacción (sus monedas). Las monedas son almacenadas en la cadena de bloques en forma de salidas de transacción.

Debido a la necesidad la clave privada correspondiente a la clave pública para utilizar los bitcoins recibidos, es necesario realizar *back ups* del monedero, ya que la pérdida de este conlleva la imposibilidad de acceder a los bitcoins asociados a esas claves, por lo que se perderán para siempre.

El cliente completo Bitcoin Core instalado genera en la carpeta raíz un archivo llamado *"wallet.dat",* es decir, el monedero personal con las claves del usuario, por lo que dada la frecuencia con la que se ven afectados los OS de Windows y la importancia de este archivo, es aconsejable cifrar el monedero y crear una copia de seguridad con cierta frecuencia. Por experiencia personal, durante la realización de este proyecto, el portátil con el que se desarrolló el proyecto se vio afectado por un ransomeware que encriptó todos los archivos del ordenador dejándolos con una extensión "*.crypt"*, obligando a la restauración del mismo con la consiguiente pérdida del archivo wallet.dat. Gracias al almacenamiento de todos los archivos en una memoria USB los daños no fueron reseñables. Para recuperar el monedero se necesita únicamente volver a copiar el archivo en la ruta en la que está instalada el cliente y reiniciarlo.

Por otro lado, vista la importancia de este archivo es prácticamente imprescindible **cifrar** el monedero con una contraseña robusta (mayor de 12 caracteres) para evitar que, en caso de pérdida o robo, no se pueda hacer uso de las claves que posibilitan el acceso a las monedas.

A continuación, mediante el cliente bitcoin core y la siguiente instrucción encripto mi monedero:

```
>>walletpassphrase [password] [timelimit]
```

O haciendo uso de la interfaz gráfica del cliente *Bitcoin Core.*

A partir de ahora, en tiempo de ejecución, el cliente carga la cartera como lo haría normalmente, sin embargo, el almacén de claves contiene las claves de forma cifrada. Cuando se quiere hacer uso del monedero mediante alguno de los siguientes comandos: `sendtoaddress`, `sendfrom`, `sendmany`, y`keypoolrefill`devuelve el siguiente mensaje de error. Ejemplo:

```
sendtoaddress "1M72Sfpbz1BPpXFHz9m3CdqATR44Jvaydd" 0.1

Error: Please enter the wallet passphrase with walletpassphrase
first. (code -13)
```

Como ya se ha mostrado anteriormente, un monedero que no esté protegido con una contraseña puede ser fácilmente accesible por un atacante simplemente substrayendo el fichero *wallet.dat*, y, por ende, dispone del par de claves necesaria para transferirse todos los bitcoins del monedero. Por otro lado, si el fichero está encriptado se dificulta el acceso al contenido de la cartera, pero no garantiza inmunidad frente ataques.

A continuación, voy a realizar unos casos de prueba para intentar desencriptar el fichero de la wallet y acceder al contenido del mismo. Para ello, haré uso del software de "Thegrideon", cuya herramienta se llama "*Bitcoin passwordrecovery".* Se basa en varios ataques que pueden ser configurados; ataques mixtos avanzados para una configuración precisa del rango de búsqueda, ataques de fuerza bruta basados en un conjunto de caracteres y longitud y ataques de diccionario.

Para la primera prueba realizo una con una contraseña notablemente débil para intentar demostrar la importancia de una contraseña robusta para garantizar la seguridad de los activos que protege la billetera.

Nota: Cómo elegir una contraseña fuerte [64].

Debe elegirse al menos un carácter de cada grupo

```
Minúsculas: abcdefghijklmnopqrstuvwxyz
Mayúsculas: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Número: 1234567890
Símbolo: `~!@#$%^&*()-_=+\|[{]};:'",<.>/? (espacio)
```

```
<9 caracteres = inaceptable
09 caracteres = inseguro
10 caracteres = seguridad baja
11 caracteres = seguridad media
12 caracteres = seguridad buena (suficientemente buena para el monedero)
13 caracteres = seguridad excelente, válida para cualquier uso.
```

Ilustración 22. Cómo elegir una contraseña fuerte [64]

- Contraseña 1: “password”

```
>>walletpassphrase "password"
```

Una vez encriptado lo introducimos en el programa, Open ->Select File (figura 26)

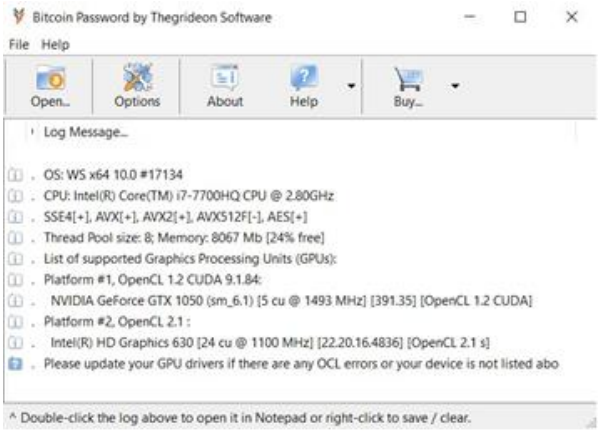


Ilustración 24. Ejecución del programa bitcoin passwordrecovery (1)

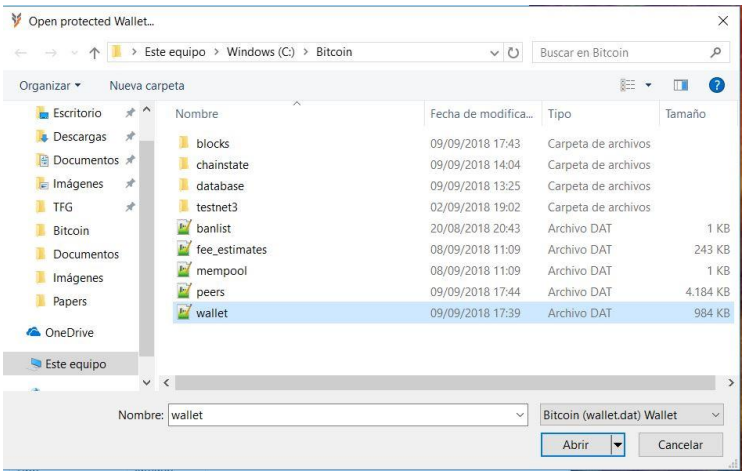


Ilustración 23. Selección del archivo wallet.dat

Como se puede apreciar, la cantidad de password por segundo depende de la capacidad computacional del ordenador, en este caso en concreto, el ordenador se trata de un Lenovo Legion Y520 con NVIDIA GTX 1050 con 4 GB de RAM dedicada, lo que permite un máximo de 833 p/s

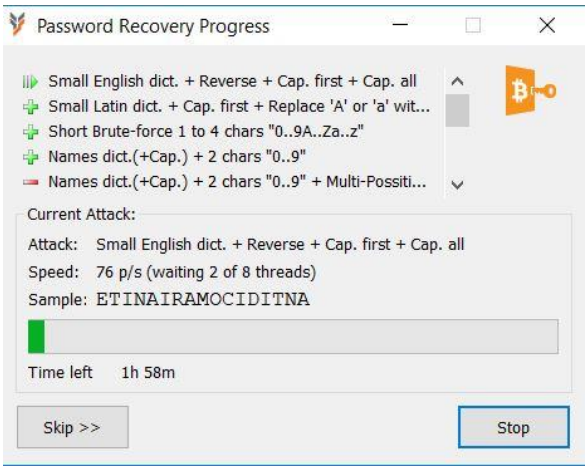


Ilustración 25. Ejecución del programa Bitcoin passwordrecovery (2)

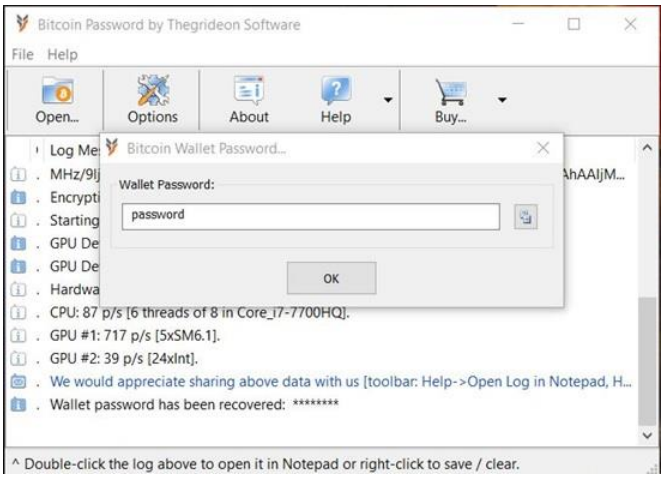


Ilustración 26. Mensaje de éxito al recuperar la contraseña

Efectivamente el programa encuentra la contraseña en 16,31 minutos.

- Contraseña 2: “Cookie21”

De nuevo proceso a encriptar el monedero, por lo que se elimina el archivo encriptado y se realiza una importación del wallet.dat sin protección, al reiniciar el cliente bitcoin core y ya reconoce de nuevo el monedero.

```
>>walletpassphrase "Cookie21"
```

En esta ocasión el resultado es el mismo, el programa después de una ejecución de 4,31 horas.

Como se puede observar las contraseñas no cumplen los requisitos de seguridad expuestos anteriormente, por lo que en la siguiente prueba se introduce una que sea considerada robusta, con una longitud de 12 caracteres e incluyendo un carácter de cada grupo [63].

- Contraseña 3: “#!TemPoral.20”

```
>>walletpassphrase "#!TemPoral.20"
```

En este caso, después de una ejecución durante 48 horas el programa finaliza su ejecución sin éxito, sin embargo, esto no significa que la contraseña sea totalmente segura; un atacante con gran poder computacional y probando este tipo de ataque durante semanas probablemente acabaría consiguiendo descifrar el fichero.

5.2 Obtención de IP´s

A pesar de que las direcciones IP no son almacenadas en el Blockchain de Bitcoin, cabe la posibilidad de obtener las direcciones usadas en una transacción. La manera más sencilla de hacer esto es correr el cliente de Bitcoin y conectarte a tantos nodos como sea posible como demuestra *Dan Kaminsky*en el paper *"Black Hat"* [65]. Siendo un sistema entre pares, si alguien es capaz de conectarse con todos los nodos del sistema será capaz siempre de identificar el primer nodo que notifica una transacción y relacionar su IP con la transacción en particular.

Se debe tener en cuenta que la mayoría de las direcciones IP de los usuarios no son estáticas y pueden cambiar con el tiempo, pero si varias transacciones son hechas con el mismo IP en un corto espacio de tiempo, se puede asumir que esas transacciones han sido hechas por el mismo usuario.

Mediante el uso del comando `getpeerinfo` del cliente Bitcoin obtenemos datos de cada nodo como una lista de objetos json:


```
[
{
    "id": 755,
    "addr": "213.174.156.83:8333",
    "addrlocal": "85.58.144.40:17006",
    "addrbind": "192.168.1.142:57484",
    "services": "000000000000040d",
    "relaytxes": true,
    "lastsend": 1536514229,
    "lastrecv": 1536514238,
    "bytessent": 4571,
    "bytesrecv": 35768110,
    "conntime": 1536513276,
    "timeoffset": -39,
    "pingtime": 0.117848,
    "minping": 0.117848,
    "version": 70015,
    "subver": "/Satoshi:0.16.0/",
    "inbound": false,
    "addnode": false,
    "startingheight": 540675,
    "banscore": 0,
    "synced_headers": 540677,
    "synced_blocks": 457294,
    "inflight": [
        …
    ],
```

```
    "whitelisted": false,
    "bytessent_per_msg": {
      "addr": 265,
      "feefilter": 32,
      "getaddr": 24,
      "getdata": 2797,
      "getheaders": 1053,
      "ping": 64,
      "pong": 96,
      "sendcmpct": 66,
      "sendheaders": 24,
      "verack": 24,
      "version": 126
    },
    "bytesrecv_per_msg": {
      "addr": 30442,
      "block": 35651764,
      "feefilter": 32,
      "getheaders": 1053,
      "headers": 318,
      "inv": 83376,
      "ping": 96,
      "pong": 64,
      "sendcmpct": 66,
      "sendheaders": 24,
"verack": 24,
      "version": 126
    }
  },

[…]
]
```


Como se puede apreciar, el primer campo devuelto por la consulta es la dirección IP de uno de los 8 nodos a los que se conecta el cliente automáticamente cuando se inicia; a partir de ahí, se puede tratar de sacar algún tipo de información.

A continuación, se muestra la ejecución del comando “traceroute” para mostrar la ruta que siguen los paquetes cuando buscamos la dirección IP del nodo destino

```
C:\Users\usuario>tracert 213.174.156.83

Traza a 213.174.156.83 sobre caminos de 30 saltos como máximo.

1  1608ms    12 ms    14 msliveboxplus [192.168.1.1]
  2     *        *        5 ms  10.255.2.58
  3   829 ms     7 ms    12 ms  10.255.140.45
4  2439ms    10 ms     8 ms  10.34.194.5
  5 7 ms 13 ms  6ms  bundle-ether4-14.madtr2.madrid.opentransit.net [193.251.247.13]
  6 7 ms 7 ms   6 ms  hundredgige0-1-0-2.madtr3.madrid.opentransit.net [193.251.133.131]
  7     6 ms     8 ms     7 ms  be5511.ccr32.mad05.atlas.cogentco.com [130.117.15.1]
  8    11 ms    11 ms    11 ms  be3358.ccr52.bio02.atlas.cogentco.com [130.117.1.98]
9  2694ms    32 ms    39 ms  be3324.ccr42.par01.atlas.cogentco.com [130.117.2.66]
 10   100 ms    99 ms    95 ms  be3628.ccr42.jfk02.atlas.cogentco.com [154.54.27.169]
 11   103 ms   102 ms   107 ms  be2807.ccr42.dca01.atlas.cogentco.com [154.54.40.110]
 12   119 ms   117 ms  2772ms  be3084.ccr41.iad02.atlas.cogentco.com [154.54.30.66]
 13   117 ms   120 ms   117 ms  38.122.62.114
14  1903ms   117 ms   117 ms
Traza completa.
```

Después de obtener el nombre de los host por los que pasa el paquete antes de llegar al destino, haciendo uso de un localizador de IPs [66] (software gratuito de internet) devuelve información sobre la situación geográfica (figura 22) del proveedor de servicios y el nombre del ISP (DataWeb Global Group).

IP Locator & IP Lookup Basic Tracking Info	
IP Address:	213.174.156.83 [IP Blacklist Check]
Reverse DNS:	** server can't find 83.156.174.213.in-addr.arpa: SERVFAIL
Hostname:	213.174.156.83
Address Location For IP: 213.174.156.83	
Continent:	North America (NA)
Country:	United States (US)
Capital:	Washington
State:	Virginia
City Location:	Ashburn
Postal:	20147
Area:	703
Metro:	511
ISP:	DataWeb Global Group B.V.
Organization:	DataWeb Global Group B.V.
AS Number:	AS39572 DataWeb Global Group B.V.
something went wrong!	something went wrong!
Time Zone:	America/New_York
Local Time:	02:50:27
Timezone GMT offset:	-14400
Sunrise / Sunset:	06:47 / 19:25

Ilustración 27. Localización IP nodo Bitcoin Core

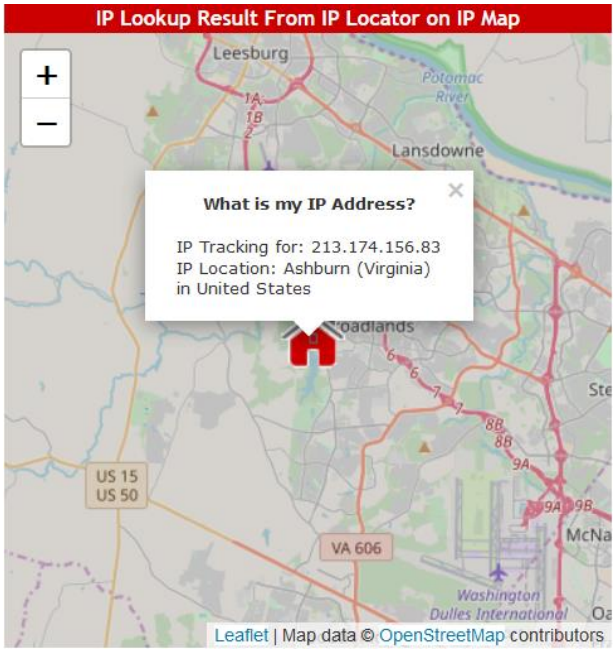


Ilustración 28. Localización IP nodo Bitcoin Core

Por otro lado, en el campo `"addrlocal"` se muestra la dirección ip del cliente instalado en nuestro equipo `"85.58.144.40"`, así, realizando el mismo proceso que en el caso anterior, se obtiene la localización de dicha ip:

IP Locator & IP Lookup Basic Tracking Info

IP Address:	85.58.144.40 [IP Blacklist Check]
Reverse DNS:	40.144.58.85.in-addr.arpa
Hostname:	40.pool85-58-144.dynamic.orange.es
Nameservers:	dns4.wanadoo.es >> 62.36.243.5 dns1.wanadoo.es >> 62.37.237.140

Address Location For IP: 85.58.144.40

Continent:	Europe (EU)
Country:	Spain (ES)
Capital:	Madrid
State:	Madrid
City Location:	Madrid
Postal:	28002
ISP:	Orange Espana
Organization:	Orange Espana
AS Number:	AS12479 Orange Espagne SA
something went wrong!	something went wrong!
Time Zone:	Europe/Madrid
Local Time:	17:59:44
Timezone GMT offset:	7200
Sunrise / Sunset:	07:58 / 20:20

La localización real donde se ha establecido el cliente de prueba con el que se realiza la petición está situada exactamente en la Ciudad de los Ángeles, distrito de Villaverde. Como se puede apreciar, la trazabilidad de la dirección IP local obtenida acaba en la puerta del Sol, que pertenece al proveedor de servicios contratado (Orange España).

En Europa, el 25 de mayo de 2018, entró en vigor una nueva ley de protección de datos (GDPR), la cual afecta a todas las empresas (independientemente de la nacionalidad) que recopilan y gestionan datos de los ciudadanos de la Unión Europea, cualquier información que pueda usarse para relacionar directa o indirectamente a una persona física.

Atendiendo estrictamente a la política de privacidad de Orange, basada en el cumplimiento de las obligaciones derivadas de la Ley de conservación de datos 25/2007 "*Orange conservará la información de tráfico y localización durante un plazo de 12 meses con el objetivo de cumplir con el deber de información en caso de recibir un requerimiento de la Autoridad Judicial*" [66].

Por tanto, se puede concluir que el único usuario capaz de conocer la situación exacta del cliente de Bitcoin es aquel que consiga acceso a los "*logs files*" (archivos que registran las transacciones de un servidor web) del ISP.

Una de las alternativas más eficientes para enmascarar la dirección IP e incluir a la red un bloqueo geográfico, es el uso de un servicio VPN; lo que proporciona una capa extra de seguridad añadiendo además un cifrado de los paquetes que se transmiten. Es especialmente importante cerciorarse que el servicio VPN que se va a utilizar no almacena logs, algo que puede resultar una tarea ardua, especialmente en los servicios gratuitos que ofrecen, como bien indica el experto en seguridad Chema Alonso "La gente tiene que entender que Internet no es gratis: pagas con tus datos".

Los servicios VPN que ofrecen mejores prestaciones son de pago, por lo que otra opción es el uso de la red Tor.

6. BLOCKCHAIN VS BASE DE DATOS TRADICIONAL

Las bases de datos tradicionales siguen una arquitectura de red cliente-servidor; un usuario (conocido como cliente) puede modificar los datos según unos criterios de permisos establecidos que se almacenan en un servidor centralizado. El control de la base de datos permanece bajo la jurisdicción de una autoridad designada, que certifica las credenciales de un cliente antes de facilitar el acceso a la base de datos. Debido a que el administración y control de la base de datos depende de dicha autoridad, si la seguridad de la autoridad se ve comprometida, los datos pueden modificarse o incluso eliminarse.

La base de datos de Blockchain depende de la honestidad de los nodos descentralizados que conforman la red. Cada nodo participa en la gestión; todos los nodos verifican nuevas transacciones que se adhieren al *blockchain*, y son capaces de ingresar nuevos datos en la base de datos. Para que se realice el sellado de los bloques, la mayoría de los nodos deben estar de acuerdo, es decir llegar a un consenso. Este mecanismo de consenso garantiza la seguridad de la red, debido a que para que se produzcan manipulaciones en la base de datos se debe dar un número de nodos deshonestos mayor al 51%, lo que dificulta su manipulación.

6.1 Blockchain SQL

Haciendo uso del software gratuito de Blockchainsql [70] que almacena el blockchain de bitcoin en una base de datos SQL permite hacer consultas directas al blockchain mediante una estructuración muy completa, distribuida en tablas, que almacena los datos como se muestra continuación:

Table Name	Column Name	Column Position	Column Type
AddressType	ID	1	SMALLINT
AddressType	Name	2	VARCHAR
AddressType	Description	3	NVARCHAR
Block	ID	1	INT
Block	Height	2	INT
Block	PreviousBlockHash	3	BINARY
Block	Hash	4	BINARY
Block	BranchID	5	INT
Block	Size	6	BIGINT
Block	Nonce	7	BIGINT
Block	TimeStampUnix	8	BIGINT
Block	TimeStampUtc	9	DATETIME
Block	MerkleRoot	10	BINARY
Block	Bits	11	BIGINT
Block	Difficulty	12	REAL
Block	Version	13	INT
Block	TransactionCount	14	BIGINT
Block	OutputsBTC	15	DECIMAL
Block	RewardBTC	16	DECIMAL

Ilustración 30. Estructura de las tablas blockchainsql

De esta manera, sin la necesidad de almacenar la cadena de bloques completa (184 Gb a día de hoy), se pueden intentar mirar ciertos aspectos que puedan ser usados para inferir información privada del dueño u otros aspectos curiosos del registro histórico de transacciones y bloques del blockchain.

Por un lado, se obtendrá un análisis probabilístico en relación al número de entradas que tiene de media una transacción:

```
SELECT AVG(InputCount) AS InPutAverage FROM [Transaction]
```

2

El número medio de entradas en una transacción corresponde a 2, esto tiene sentido ya que como ya la cantidad de bitcoins a la que hace referencia la entrada generalmente no será igual a la cantidad que un usuario desea enviar. Como las entradas sólo se pueden usar una vez, se debe crear una nueva salida para devolver el cambio; por lo que, a su vez, en común ver dos entradas para hacer un pago a una dirección, referidas a direcciones de cambio de pagos anteriores; por lo que se puede inferir que las dos entradas corresponden normalmente al mismo usuario, aunque no tiene por qué ser así siempre.

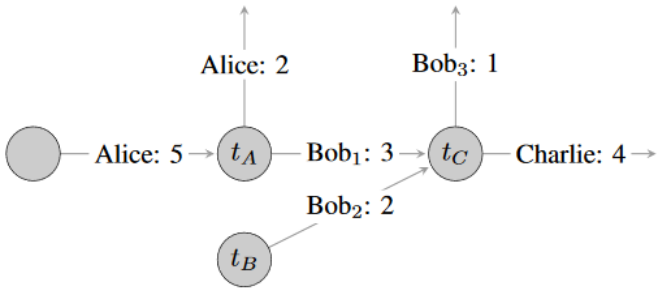


Ilustración 31. Ejemplo de un grado de transacción parcial [68]

En el siguiente gráfico, obtenido mediante la consulta iterada sobre el número de entradas, se muestra de forma exacta el porcentaje del número de entradas en una transacción desde el bloque génesis (bloque que contiene la primera transacción realizada en bitcoin).

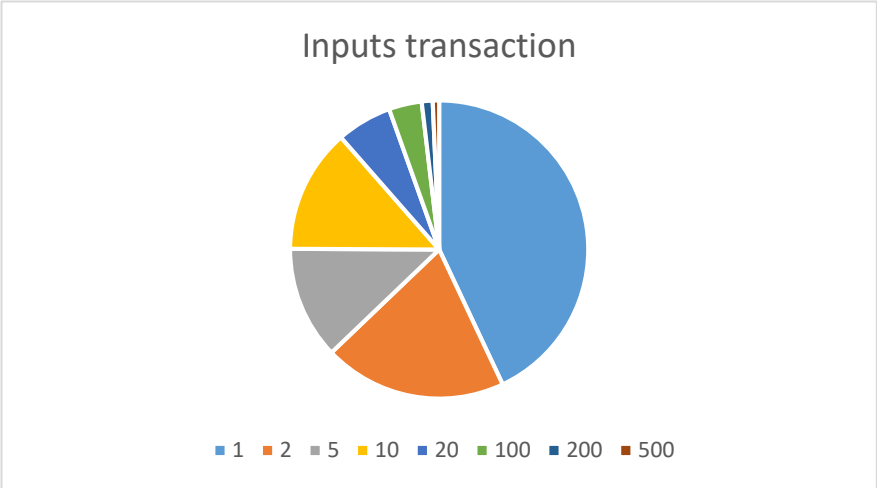


Ilustración 32. Número de entradas en una transacción

Cada transacción conlleva unas cuotas a pagar al minero por llevar a cabo el sellado del bloque y de esa manera confirmar la transacción que se ha realizado (una transacción se considera segura después de 6 confirmaciones). Es posible elegir la cuota que se desea pagar al minero, de tal forma, cuanto más dinero ofrezcas, mayor será la prioridad del minero por sellar tal transacción y, por ende, más rápido será confirmada. Al llevar a cabo la consulta sobre la transacción en la que mayor cuota de pago se ha establecido se obtiene un resultado cuanto menos curioso:

```
SELECT MAX(FeeBTC) AS MaxFee FROM [Transaction]
```

```
291.2409 BTC
```

Lo más curioso de esta consulta es que la salida de la transacción es de 0.0001 BTC, por lo que es fácil inferir que fue una confusión entre la salida y las tasas a pagar por la transacción

TXID	CC455AE816E6CDAFDB58D54E35D4F46D860047458EACF1C7405DC634631C570D
Size	1963 bytes
Block	409008
Index	1
Input Count	13
Inputs	291.241 (฿)
Output Count	13
Outputs	0.0001 (฿)
Fee	291.2409 (฿)
Lock Time	0
Version	1

Por último, mediante la siguiente consulta y especificando el ID TX se obtiene los scripts de entrada de una transacción, su valor, y la traducción del Script que se ha emitido.

```
SELECT
    O.[Name] Name,
SI.[DataLE]
    Data,
TXT.[en] Txt
FROM
    [Transaction] T INNER JOIN
TransactionInput TXI ON T.ID = TXI.TransactionID INNER JOIN
    Script S ON S.ID = TXI.ScriptID INNER JOIN
ScriptInstruction SI ON S.ID = SI.ScriptID INNER JOIN
OpCode O ON SI.OpCode = O.ID INNER JOIN
    [Text] TXT ON O.[Description] = TXT.Name
WHERE
T.TXID = 0x67F222EF921D8021EB740A87AE0A52637568E96D7FCC2DA78EE6FB167B08FCF9 AND
-- TXID (prefico con 0x) - ejemplo
TXI.[Index] = 0     -- Input index
```

Name	Data	Txt
OP_PUSHBYTES03	4F5906	The next 3 bytes is data to be pushed onto the stack
OP_0		An empty array of bytes is pushed onto the stack. (This is not a no-op: an item is added to the stack.)
OP_PUSHBYTES04	DA6B5E57	The next 4 bytes is data to be pushed onto the stack
OP_PUSHBYTES04	A086FA25	The next 4 bytes is data to be pushed onto the stack
OP_PUSHBYTES12	CE015A57C676000000000000	The next 12 bytes is data to be pushed onto the stack
OP_PUSHBYTES10	2020202020200A2F7265	The next 10 bytes is data to be pushed onto the stack
OP_IFDUP		If the top stack value is not 0, duplicate it.
OP_VERIF		Transaction is invalid even when occuring in an unexecuted OP_IF branch
OP_2SWAP		Swaps the top two pairs of items.
OP_DUP		Duplicates the top stack item.

Ilustración 33. Scripts de entrada en una transacción

7. MONEDAS ALTERNATIVAS

Debido al aumento del volumen de los datos de fácil acceso se incrementa la demanda de privacidad, los usuarios de criptomonedas comenzaron a buscar otras monedas digitales que pudieran llenar el agujero de privacidad que Bitcoin no puede cubrir. Las monedas digitales como Dash y Monero proporcionan complejas técnicas de anonimato que oscurecen las transacciones y las partes involucradas en estas transacciones. Otra moneda digital, ZCash, parece proporcionar un nivel aún mayor de fungibilidad al permitir que sus usuarios permanezcan completamente anónimos.

Dash incorpora técnicas de CoinJoin en sus transacciones" PrivateSpend*"*; Monero utiliza firmas de anillo para permitir a los usuarios crear "mezclas" (es decir, incluir las claves de otros usuarios en sus propias transacciones como una forma de proporcionar un conjunto de anonimato mayor); y Zcash utiliza las denominadas pruebas de conocimiento cero para permitir a los usuarios gastar monedas sin revelar qué monedas se están gastando.

7.1 Zcash

Zcash es una criptomoneda creada el 29 de octubre de 2016 con el objetivo de preservar la privacidad. Comparado con Monero, la privacidad de Zcash se basa en pruebas de conocimiento cero (*zero-knowledge proofs)* llamadas zk-SNARK. La estructura de Zcash es similar a la de Bitcoin, ya que la versión original de Zcash se planeó para ser una extensión del protocolo de bitcoins. El tiempo de generación de bloque es de 2,5 minutos (a diferencia de los 10 minutos de Bitcoin) y "*Equihash"* como función de prueba de trabajo. La recompensa minera actual es de 12,5 ZEC/bloque, 10 ZEC van dirigidos al minero que selló el bloque y 2,5 ZEC a los desarrolladores de Zcash como "recompensa del fundador". Dicha transacción de denomina transacción Coinbase; después de cuatro años la recompensa de la minería se reducirá a 6,25 ZEC, pero todo se destinará al minero.

La moneda en el blockchain se llama ZEC, mientras que el valor más pequeño posible es 1 Zatoshi, donde 1 ZEC = 108 Zatoshi. La tarifa de transacción predeterminada es de 104 Zatoshi. El suministro total de ZEC será ligeramente inferior a 21 millones, que es el mismo que en Bitcoin. La minería se realiza principalmente por *pools*de minado, donde el umbral promedio para los pagos es 106 Zatoshi.

7.1.1 Transacciones

En general, hay dos tipos de transacciones en Zcash. Los primeros son transacciones transparentes; estas transacciones funcionan de la misma manera que una transacción de bitcoin, con salidas no utilizadas como entradas, y las nuevas salidas no gastadas como salidas de la transacción, mientras que la diferencia entre el valor total de las entradas y salidas es la tarifa de transacción. Solo pueden transferir monedas entre direcciones públicas o transparentes (t), ya que en blockchain la clave pública de estas direcciones siempre comienza con una "t". Estas transacciones también se conocen como transacciones t-to-to.

El segundo tipo de transacciones son las transacciones que están enviando o recibiendo monedas desde una dirección oculta, y la clave pública para estas direcciones siempre comienza con una "z". Una transacción puede usar direcciones t y z, pero la dirección z no es revelada en la cadena, sólo una prueba de que hay una dirección z válida, que envió o recibió la cantidad desconocida de monedas. Se denomina comúnmente "*JoinSplit*" o "JS" a todas las transacciones que implica una dirección-z [60].

Puede haber 4 transacciones *JoinSplit* diferentes en general [59]:

- Transacciones z-to-z: el caso más simple se produce cuando no hay entrada o salida pública, lo que significa que la transferencia es sólo entre direcciones z. Las únicas nuevas monedas reveladas en el campo "Vpub view" son las tarifas de transacción.
- Transacciones z-to-t: en estas transacciones no hay entrada pública, pero hay al menos una producción pública, donde la suma de las salidas tiene que ser menor o igual a las nuevas monedas reveladas, mientras que el resto es la tarifa de transacción.
- Transacción t-to-z: en este caso, no hay salidas públicas en una transacción, sólo entradas públicas. La suma de las entradas debe ser mayor o igual a la cantidad de monedas ocultas, mientras que el resto es la tarifa de la transacción.
- Transacciones tz-to-tz: el último caso, en el que participa *joinsplit*, pero también hay entradas y salidas públicas en la transacción. En este caso, la tarifa de transacción es la diferencia entre las monedas recientemente reveladas de las uniones y la suma de las salidas públicas.

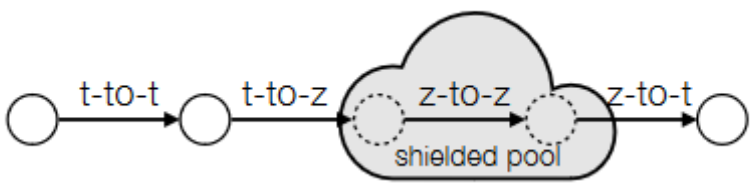


Ilustración 34. Tipo de transacciones [59]

7.1.2 Funcionamiento de Zcash

Zcash (ZEC) es una criptomoneda alternativa desarrollada como un *fork* de Bitcoin que pretende romper el vínculo entre remitentes y destinatarios en una transacción. En Bitcoin, los destinatarios reciben fondos en direcciones (lo que se conoce como Vout en una transacción), y cuando los gastan lo hacen desde estas direcciones (a las que se hace referencia como Vin). El hecho de gastar bitcoins crea así un vínculo entre el emisor y el destinatario, y estos enlacen se pueden seguir a medida que los bitcoin continúan cambiando de manos. Por lo tanto, es posible rastrear cualquier Bitcoin desde si creación hasta su propietario actual.

Cualquier transacción que interactúe con el llamado pool blindado en Zcash lo hace a través de la inclusión de un vJoinSplit, que especifica de donde vienen las monedas y hacia dónde se dirigen. Para recibir fondos, los usuarios pueden proporcionar una dirección transparente (dirección t) o una dirección blindada (dirección z). Se dice que las monedas que se mantiene en direcciones z están en el grupo blindado. Para especificar a dónde van los fondos, un vJoinSplit contiene:

- Una lista de direcciones t de salida con fondos asignados a ellas (llamadas Zout)
- Dos salidas blindadas
- Un campo memo encriptado. El Zout puede estar vacío, en cuyo caso la transacción está blindada (t-to-z) o privada (z-to-z), dependiendo de las entradas.

Si la consideramos que está vacía (ya que esta es simplemente la asignación de la tarifa del minero). Cada salida blindada contiene una cantidad desconocida de ZEC, así como un token oculto de doble gasto. La salida blindada puede ser una salida ficticia (es decir, contiene cero ZEC) para ocultar el hecho de que no hay salida tapada. El campo memo cifrado se puede usar para enviar mensajes privadas a los destinatarios de las salidas blindadas [59] [60].

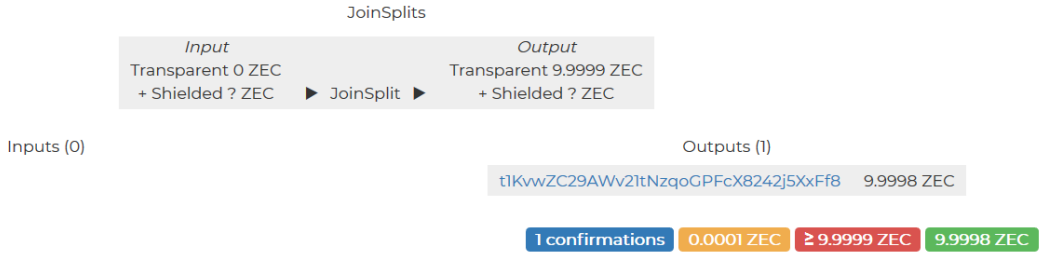


Ilustración 35. Ejemplo de transacción en Zcash

Para especificar de dónde provienen los fondos, un vJoinSplit también contiene una lista de t-direcciones de entrada (llamadas Zin), dos token de doble gasto y una prueba de conocimiento cero. El Zin puede estar vacío, en cuyo caso la transacción está protegida (z-to-t) si Zout no está vacía, o privado (z-to-z) si lo está [59]. Cada token de doble gasto es una token único que pertenece a alguna salida apantallada anterior, o un valor ficticio utilizado para ocultar el hecho de que no hay entrada blindada.

8. CONCLUSIONES

A la vista de la investigación y de los resultados obtenidos se puede determinar que Bitcoin no es anónimo; entendiendo como anonimato lo siguiente: "*Dicho de una persona indiferenciada: De nombre desconocido o que se oculta".* Ciñéndose a la estricta definición de la palabra no es posible afirmar con totalidad que se trate de un servicio anónimo. De hecho, han surgido nuevas compañías dedicadas al análisis forense de la cadena de bloques con el fin de obtener información personal en determinadas ocasiones como ChainAnalysis, la cual, fue decisiva en el arresto del cibercriminal ruso "Alexander Vinnik", que, según el departamento oficial de justicia, ayudó a lavar más de 4 billones de dólares a criminales.

Existen mecanismos que ayudan a ofuscar la trazabilidad de las transacciones, como los mixers los cuáles proporcionan un mayor nivel de anonimato a cambio de una tarifa, aproximadamente un 3% del total del dinero a lavar. Aun así, es necesario conocer la reputación del servicio ya que es necesario confiar en su integridad, ya que por una parte se le otorga la posesión de los bitcoins, y por otro lado es necesario que no guarde un registro de su actividad, ya que, si una tercera persona accede a esa información, la ofuscación de la trazabilidad desaparece.

Es importante mantener un alto nivel de seguridad y precaución con el monedero; la manera más óptima de almacenar los Bitcoin es en el monedero de un cliente completo donde el usuario es el encargado de la íntegra seguridad del mismo, por ende, esto se traduce en un especial cuidado a la hora de realizar operaciones y almacenarlo. Es importante realizar copias de seguridad, con una frecuencia relativa en función del número de transferencias que realiza el usuario, por otro lado, y de igual o mayor importancia es el cifrado del monedero, ya que de manera contraria cualquier atacante que se haga con el archivo podrá hacer uso de las claves privadas del mismo simplemente importándolo en su propio sistema. Aun aplicando cualquier medida de seguridad nunca se está completamente seguro mientras el dispositivo que lo almacena esté conectado a la red ya que ha quedado demostrado que se puede des-encriptar un monedero si la contraseña establecida por el usuario no es lo suficientemente robusta, por tanto, es altamente recomendable el uso de carteras en frío.

Por último, hacer mención de un resumen de posibles métodos descritos en el trabajo que pueden otorgar un mayor anonimato al hacer uso de esta tecnología; uso de mixers, navegador Tor, uso de VPN, crear nuevas direcciones por cada transacción, JoinMarkets o incluso la compra física de bitcoins en locales habilitados. [67].

9. FUTURAS LÍNEAS DE INVESTIGACIÓN

El trabajo ha contribuido a resolver incógnitas sobre ciertos aspectos de esta innovadora tecnología, pero a su vez ha generado nuevas inquietudes sobre el tema y ha abierto sugerentes líneas de investigación que se expondrán en a continuación en el siguiente apartado.

Desde el punto de vista del protocolo Bitcoin y el medio ambiente el algoritmo de prueba de trabajo que se utiliza para verificación de bloques es ecológicamente insostenible debido al exponencial poder computacional requerido debido al aumento de la dificultad en el sellado de bloques; por lo tanto, una interesante línea de investigación sería el estudio de otros algoritmos de prueba de trabajo como prueba de participación ("*Proof-of-Stake*") donde la probabilidad de recibir la recompensa por sellado de bloque aumenta en función de la cantidad de monedas que uno acumula. Por otro lado, se encuentra la prueba de actividad ("*Proof-of-Activity*"), un híbrido del algoritmo de prueba de trabajo y el de prueba de participación.

De manera análoga existe la posibilidad de estudiar una cadena de bloques distinta al *blockchain* de bitcoin como puede ser la deEthereum, con opción de programar un contrato inteligente gestionado por la propia cadena de bloques y aplicarlo en algún negocio existente en la actualidad, realizando una comparativa de negocio con el dinero que se ahorraría el usuario con la ausencia de intermediarios.

Atendiendo al nivel de red del sistema sería interesante un análisis grafo de las transacciones tras usar diversos servicios de lavado con la pretensión de medir el nivel de ofuscación de las trazas que relacionan determinadas transacciones con el usuario propietario de la dirección bitcoin.

Por último, con el fin de aplicar la funcionalidad que tanto se pretende conocer, sería altamente recomendable la implicación en algún proyecto que se está llevando a cabo en la actualidad como la creación de una plataforma *Blockchain* para el registro y certificación de contenido multimedia que garantice la propiedad intelectual o la inclusión de un registro público en la creación y certificación de marcas y patentes.

10. SUMMARY

Bitcoin is an electronic currency located in a P2P payment network that operates out of any Bank or Government regulation scope. This crypto-currency runs through blockchain technology, a public register that performs through a database with a sophisticated codification system of information that stores the historic data of all transactions released. This system avoids the major issue found with other digital currencies, known as *double spending.* The fact that every user can actively participate in this network providing full transparency is a key factor given the lack of transparency in models based on third parties' confidence.

This new technology has definitely disrupted the economic and technology world over the last decade. Moreover, it is not only about developing a new technological tool it is about creating a new plural, transparent and democratic system whose main goal is the decentralization. Nowadays there are already some companies applying the collaborative-economy model like *AirBnB*, however, blockchain brings the chance to operate with no agents or brokers.

For the purpose of this project, BitCoin Core has been downloaded in a local server at university, which allowed to be part of the network that verifies transactions in blockchain. This fact will let obtain information about transactions, blocks, in addition to IP addresses between peers.

The Bitcoin protocol client is called Bitcoin Core, it is an open source software that allows the user to be part of the network as a Bitcoin node through transaction verification. In order to synchronize with the system, a complete copy of the block chain is required, currently approximately 180 Gb. This tool provides the user with a portfolio of their own, which completely verifies the payments. The complete Bitcoin Core installed client generates in the root folder a file called "wallet.dat", that is, the personal wallet with the user's keys, so given the frequency with which Windows OSs are affected and the importance of this file, it is advisable to encrypt the wallet and create a backup with some frequency.

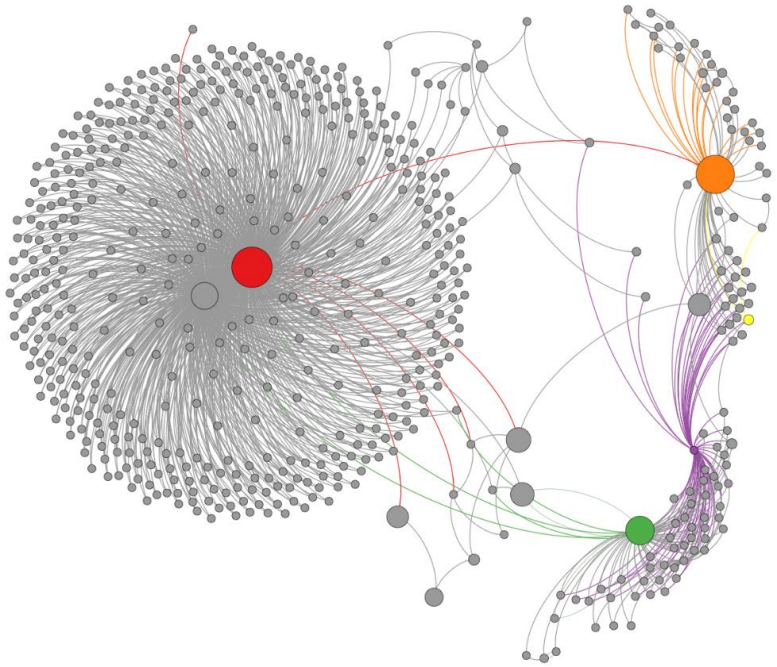
There are different types of wallets to store bitcoins each of them provides a different level of security and complexity so they are usually the target of most attacks in the system. Since it is the only part whose security is independent of the Bitcoin protocol itself. Specifically, the security of the client's wallet will be analyzed and various ways in which an attacker can get hold of the passwords of the wallet and thus make use of its funds.

Subsequently, the existing services are analyzed to mitigate protocol deficiencies at the level of anonymity, such as mixers or the use of the TOR network, with the aim of avoiding the tracking of transactions and identity in a communication between peers

through traffic analysis techniques. Due to the fact that all transactions are publicly stored in the blockchain, the anonymity of an issuer is based on the absence of any link between the pseudonym and its true identity. In general, users must provide personal information in order to buy bitcoins, so from the first moment the personal information of the user is stored on the website where the bitcoins are acquired.

Due to the fact that all transactions are publicly stored in the blockchain, the anonymity of an issuer is based on the absence of any link between the pseudonym and its true identity. In general, users must provide personal information in order to buy bitcoins, so from the first moment the personal information of the user is stored on the website where the bitcoins are acquired.

To hide the traceability there do mixers provide data obfuscation techniques, such as that, where Bitcoin users can make it difficult to trace their transactions using this technique, which combines the funds of a large number of users, mixes and sends return to different directions at various times instants and in smaller fractional quantities.



Ilustration 1. Mixer graph analisys

Mixing services usually charge a percentage of the mixed funds, approximately 3-5% of the total amount that you want to mix. In the common implementation, the mixer provides a "mix direction" that receives coins from multiple customers and sends them randomly to a new address for each client after thousands of transactions. As a

precautionary measure, it is recommended to access through Tor to hide the IP address in the event that the service stores user activity record [52].

These services are often used by malicious customers, hackers, scammers and criminals who use ransomware and threaten "Distributed Denial of Service" (DDoS) as a form of extortion in exchange for bitcoins, however, they are also used by people who are not involved in illicit or criminal activities, but want to preserve the privacy of their Bitcoin transactions. Therefore, the use of such service does not necessarily imply that the user has participated in criminal or illegal activities, in spite of this, the users of the mixers will mix their transactions with those engaged in illicit activities, contaminating the transactions.

On the other hand, at the transaction level Bitcoin is a currency whose traceability is considered high, that is why there are services such as mixers that try to break with the traces reflected in the accounting book to increase their anonymity and avoid the traceability of their activities. In order to verify this fact, queries will be made to a SQL database (StructuredQueryLanguage) in which the entire blockchain is stored to obtain certain aspects that could be used to infer private information from the owner.

Making use of the free software of Blockchainsql that stores the blockchain of bitcoin in a SQL database allows to make direct queries to the blockchain through a very complete structuring, distributed in tables that stores the data.

When making the query about the average number of entries in a transaction the result was 2, this makes sense because as the amount of bitcoins referred to by the entry will not be equal to the amount that a user wants to send. Since the entries can only be used once, a new output must be created to return the change; so, in turn, it is common to see two entries to make a payment to an address referred to exchange addresses of previous payments; so it can be inferred that the two entries correspond to the same user, although it does not always have to be that way.

Ilustration 2. Multiple input example

In the illustration 2 we can see an example of a transaction with multiple entries in which it is almost certain that the two entries correspond to the same user, one being a "UTXO" (Unspent Transaction Output), that is, an address where the change of a past transaction was sent.

Transactions are the basis of the Bitcoin protocol, since the objective of the system is to create, propagate through the network, validate and register these operations in the blockchain. They are codified and public data structures.

- **Inputs**: In order to understand how tickets work, it is essential to know what the UTXO or UTXO transactions are. The UTXO are indivisible pieces of BTC linked to a specific owner, annotated in the chain of blocks and recognized by all the participants of the network. Each time a user receives a transfer with bitcoins in their favor, it is registered in the blockchain as a UTXO. In fact, there is no concept of balance in the Bitcoin protocol, but it is a nomenclature used by the wallets to refer to the total amount of BTC that a user has in reference to the amount of UTXO that they belong to. The transaction is created from an unspent exit, the application of the wallet selects the UTXO of the user so that they compose a value equal to or greater than that of the exit [15].

- **Outputs:** recorded in the ledger, it contains the fields where the addresses to which they are to be sent are indicated and the BTC set sent to each recipient. The system of indivisible unit called Satoshi is used, which is equivalent to the cent in the Euro (1 BTC = 108Satoshis). The value of the output must always be equal to or lower than the input, never higher. For example, in the case that we have a balance of 7 BTC and we want to send 3 BTC to another user, an output of 4 BTC is created again with our address, equivalent to the transaction change [15].

Ilustration 3. Multiple output example with UTXO

In order for the transaction to be carried out, it is necessary to specify the commission that the miners will receive. These emission rates serve as an incentive to add the transaction in the next block and thus avoid abuses of the

system by de-incentivizing the "spam" of micro-transactions. They are not mandatory, transactions can be processed and included in the next block in the same way, but as the number of users increases, more operations are carried out per minute that may exceed the capacity of the network, requiring more time to process them.

Regarding the network level, although IP addresses are not stored in the Bitcoin Blockchain, it is possible to obtain the addresses used in a transaction. The simplest way to do this is to run the Bitcoin client and connect to as many nodes as possible as Dan Kaminskyen demonstrates the paper "Black Hat" [65]. Being a peer-to-peer system, if someone is able to connect with all the nodes in the system, they will always be able to identify the first node that notifies a transaction and relate their IP to the particular transaction.

It should be borne in mind that most of the IP addresses of users are not static and may change over time, but if several transactions are made with the same IP in a short period, it can be assumed that the same user has made those transactions.

It is important to maintain a high level of safety and caution with the wallet; the best way to store Bitcoin is in the wallet of a complete client where the user is in charge of the full security of the same, therefore, this translates into special care when performing operations and store it. It is important to make backup copies, with a relative frequency depending on the number of transfers made by the user. On the other hand, equal or greater importance is the encryption of the wallet, since otherwise any attacker who takes the file can make use of the private passwords of the same simply by importing it into its own system. Even applying any security measure is never completely safe while the device that stores it is connected to the network since it has been demonstrated that a wallet can be unencrypted if the password established by the user is not sufficiently robust, therefore , the use of cold wallets is highly recommended.

Finally, I would like to sum up a list of methods described over this TFG that can grant greater anonymity when using this technology: use of mixers, Tor browser, and use of VPN, create new addresses for each transaction, JoinMarkets or even the physical purchase of bitcoins in authorized locations.

11. GLOSARIO

Palabra clave	
Log	Archivo de empresa que contiene un registro de actividades de los usuarios
Exchange	Casa de compra venta de criptomonedas
IA	Inteligencia artificial
Smart contract	Contrato inteligente referido al blockchain de Ethereum
Peer-to-peer	Sistema entre pares sin intermediario
Nonce	Número aleatorio
Hashrate	Poder computacional para el cálculos de hashes
BTC	Acrónimo de Bitcoin
Spam	Envío masivo
Check sum	Suma de verificación
Double spending	Doble gasto referido a monedas digitales
Time-stamping	Mecanismo que demuestra la existencia de un archivo
PoW/PoS	Prueba de trabajo
Fork	Bifurcación de la cadena de bloques
DDoS	Ataque de denegación de servicio distribuido
Mixer	Servicio de lavado de monedas digitales
BackUp	Copia de seguridad

12. BIBLIOGRAFÍA

[1] Herrera, Carlos - "Nuevas regulaciones en Japón propician la caída abrupta del Bitcoin —esto es lo que debes saber" -*Coincrispy* - 22/07/2018 – [En línea]. Disponible en: https://www.coincrispy.com/2018/06/22/nuevas-regulaciones-japon-caida-abrupta-bitcoin/

[2] @Yúbalfm – "Las ideas que está teniendo el gobierno para regular las ICO, las criptomonedas y blockchain" – *XATAKA* – 22/02/2018 - [En línea]. Disponible en: https://www.xataka.com/criptomonedas/las-ideas-que-esta-teniendo-el-gobierno-para-regular-las-ico-las-criptomonedas-y-blockchain

[3] Durarte, Esteban – "SpanishPartyWeighsTax Incentives to Lure Blockchain Firms" – *Bloomerg* – 15/02/2018 – [Enlínea]. Disponible en: https://www.bloomberg.com/news/articles/2018-02-15/rajoy-s-party-weighs-tax-breaks-for-spanish-blockchain-companies

[4] Cabrera Valencia, Fabiola - "Tecnología Blockchain: elementos básicos,aplicaciones y marcos regulatorios" – *Biblioteca del Congreso Nacional de Chile* – 09/05/2018 – [En línea]. Disponible en: https://www.bcn.cl/obtienearchivo?id=repositorio/10221/25308/1/Bolckchain_conceptos_impacto_en_industrias_y_marcos_regulatorios_FInal.pdf

[5] Oliva León, Ricardo – "Regulación legal del bitcoin y de otras criptomonedas en España"– *Algoritmolegal* – 14/03/2018 – [En línea] – Disponible en: https://www.algoritmolegal.com/tecnologias-disruptivas/regulacion-legal-del-bitcoin-y-de-otras-criptomonedas-en-espana/

[6] BOE – "Plan Anual de Control Tributario y Aduanero de 2018" –- *cve: BOE-A-2018-792*- 23/01/2018 – [En línea] – Disponible en: https://www.boe.es/boe/dias/2018/01/23/pdfs/BOE-A-2018-792.pdf

[7]FARRÀS, Cristina; SALMERON, Adrià Morron. Del trueque a la criptomoneda: una breve historia del intercambio. *Informe Mensual-La Caixa*, 2018, no 423, p. 32-34.

[8] ORTEGA, Liliana Camacho. Bitcoin, el cambio de paradigma económico.

[9]CHAUM, David. Achievingelectronicprivacy. *Scientificamerican*, 1992, vol. 267, no 2, p. 96-101.

[10] NAKAMOTO, Satoshi. Re: Bitcoin P2P e-cash paper. *Email posted to listserv*, 2008, vol. 9, p. 04.

[11] Díaz Marco, Víctor. "Bitcoin:Plnateamiento y protocolo", 2016/04/13, [En línea] – Disponible en:https://victordiaz.me/bitcoin

[12] @ploum, “Vanity bitcoin addresses: a new way to keepyour CPU busy”, 2011/05/29, [Enlínea] – Disponibleen: https://bitcointalk.org/ index.php?topic=1387 .msg150668#msg150668

[13] CISNEROS CAMPOS, Andrés. Estudio de la red Bitcoin.

[14] ROSALES, Moisés Salinas; MALEDO, Victor Gabriel Reyes; GARCIA, Gina Gallegos. BITCOIN: UNA VISIÓN GENERAL.

[15] ANTONOPOULOS, Andreas M. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

[16] EYAL, Ittay; SIRER, EminGün. Majorityisnotenough: Bitcoin miningis vulnerable. *Communicatins of the ACM*, 2018, vol. 61, no 7, p. 95-102.

[17] DE VRIES, Alex. Bitcoin'sGrowingEnergyProblem. *Joule*, 2018, vol. 2, no 5, p. 801-805.

[18]Bitcoin EnergyConsumptionIndex. [En línea] – Disponible en: https://digiconomist.net/bitcoin-energy-consumption

[19] GroupBTC; Invierte en tu propia máquina de minado […]. 2016/20/09, [En línea] – Disponible en: https://www.groupbtc.com/es/articulo/invierte-en-tu-propia-maquina-de-minado-y-llevate-un-70-de-su-rendimiento-sin-mover-un-0

[20]STATISTICS, I. Key worldenergystatistics 2017. *International Energy Agency*, 2017.

[21] Precio KWh Europa - [En línea] – Disponible en: https://comparadorluz.com/faq/precio-kwh-electricidad/europa

[22] The bitcoin and blockchain: energyhogs, 2017/05/16, [Enlínea] – Disponibleen:http://theconversation.com/the-bitcoin-and-blockchain-energy-hogs-77761

[23] Swan, M. (2015). *Blockchain:Blueprintfor a New Economy*. Sebastopol: O'Reilly Media, Incorporated.

[24] CONTI, Mauro, et al. A surveyonsecurity and privacyissues of bitcoin. *IEEE CommunicationsSurveys&Tutorials*, 2018.

[25] H. Finney (2011), “Bestpracticeforfasttransactionacceptancehowhighistherisk?” [Enlínea] - Disponible: https:// bitcointalk.org/ index.php?topic=3441.

[26] J. Heusser, “Satsolvinganalternative to bruteforce bitcoin mining,” – [Enlínea] - Disponibleen: https:// jheusser.github.io/ 2013/ 02/ 03/ satcoin.html, 2013.

[27] C. Natoli and V. Gramoli, - [Enlínea] - Disponibleen: “The balance attack against proof-of-work blockchains: The R3 testbed as anexample,”CoRR, vol.abs/1612.09426, 2016.

[28] Wood, - [Enlínea] – Disponibleen: “Ethereum: A securedecentralisedgeneralisedtransaction-ledger,”yellow paper, 2015.

[29] J. A. Kroll, I. C. Davey, and E. W. Felten, - [Enlínea] – Disponibleen: “Theeconomics of bitcoinmining, or bitcoin in thepresence of adversaries,” 2013

[30]Decker and R. Wattenhofer, - [Enlínea]: “Bitcoin transactionmalleabilityandmtgox,” inESORICS 2014: 19th EuropeanSymposiumonResearchin Computer Security.Springer International Publishing, 2014, pp.313–326.

[31] The bitcoin malleability attack how can itunderminetheblockchainscredibility?” – Disponibleen: http:// www.coinwrite.org/, 2017

[32] Brito, J., & Castillo, A. (2013). A primer forpolicymakers.Policy: AJournal of PublicPolicy and Ideas, 29(4), 3–12

[33] Rebecca Campbell, “Uk Company Linked to theTheft of 650.000 Bitcoin from Mt Gox” – [Enlínea] – Disponibleen: https://coinjournal.net/uk-company-linked-to-the-theft-of-650000-bitcoins-from-mt-gox/ , 07/05/2018

[34] Zander, T. (2014). “Doesanyonehaveanything at allsignedbySatoshi’s PGP key?”RetrievedOctober12, 2015, [Enlínea] – Disponibleen: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-September/006621.html

[35] Van Hout, M. C., &Bingham, T. (2014). “Responsiblevendors,intelligentconsumers: Silk Road, the online revolution inCryptocurrencies and Business Ethicsdrugtrading.International Journal of DrugPolicy”, 25, 183–189.

[36] DIERKSMEIER, Claus; SEELE, Peter. Cryptocurrencies and businessethics. *Journal of Business Ethics*, 2016, p. 1-14.

[37] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, “Game-theoreticanalysis of ddosattacksagainst bitcoin mining pools,” in FinancialCryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC 2014,.SpringerBerlin Heidelberg, 2014, pp. 72–86

[38] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, “Proof of activity: Extendingbitcoin’s proof of work via proof of stake [extended abstract]y,” SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34–37, Dec. 2014.

[39] C. Decker and R. Wattenhofer, “A fast and scalablepayment network with bitcoin duplexmicropaymentchannels,” in Stabilization, Safety, and Security of

DistributedSystems: 17th International Symposium, SSS 2015. Springer International Publishing, 2015

[40] BONNEAU, Joseph, et al. Mixcoin: Anonymityfor Bitcoin withaccountable mixes. En International ConferenceonFinancialCryptography and Data Security. Springer, Berlin, Heidelberg, 2014. p. 486-504.

[41] Moser, M.: Anonymity of Bitcoin Transactions: AnAnalysis of MixingServices.In: Proceedings of M¨unster Bitcoin Conference (2013)

[42] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, "Tamperingwiththedelivery of blocks and transactions in bitcoin," in Proceedings of the 22Nd ACM SIGSAC ConferenceonComputer and Communications Security, ser. CCS '15. ACM, 2015, pp. 692–705.

[43] K. Liao, Z. Zhao, A. Doupe, and G. J. Ahn, "Behindcloseddoors: measurement and analysis of cryptolockerransoms in bitcoin," in 2016 APWG SymposiumonElectronicCrimeResearch (eCrime), June 2016, pp. 1–13.

[44] M. Kiran and M. Stannett, "Bitcoin riskanalysis,"Available:http:// www.nemode.ac.uk/wp-content/ uploads/2015/02/2015-Bit-Coin-risk-analysis.pdf , Dec. 2014.

[45] B. Masooda, S. Beth, and B. Jeremiah, "Whatmotivatespeople to usebitcoin?" in Social Informatics: 8th International Conference, SocInfo2016. Springer International Publishing, 2016, pp. 347–367.

[46] Mike Small CEng, "Blockchain and Risk", 20/04/2016, [Enlínea] – Disponibleen: https://m.isaca.org/chapters8/Northern-England/Events/Documents/blockchain.pdf

[47] MIERS, Ian, et al. Zerocoin: Anonymousdistributed e-cash from bitcoin. En *Security and Privacy (SP), 2013 IEEE Symposiumon*. IEEE, 2013. p. 397-411

[48] Dª Belén Veleiro Reboredo, "El Reglamento UE sobre protección de datos y las comunidades de propietarios", 01/06/2018, [En línea] – Disponible en: https://www.elderecho.com/tribuna/civil/Reglamento-UE-Proteccion-Datos-Comunidades-Propietarios_11_1232305005.html

[49] MOSER, Malte. "Anonymity of bitcoin transactions". 2013

[50] https://www.coinbase.com/signup

[51] A. P_tzmann and M. Hansen. A terminologyfortalkingaboutprivacyby data minimization: Anonymity, Unlinkability,Undetectability, Unobservability, Pseudonymity,and Identity Management, 2010.

[52] YANG, Danny; GAVIGAN, Jack; WILCOX-O'HEARN, Zooko. Survey of confidentiality and privacypreservingtechnologiesforblockchains. *R3, Zcash Company, Res. Rep*, 2016

[53] https://forkdrop.io/#table-bitcoin

[54] http://crypsys.mmci.uni-saarland.de/projects/CoinShuffle/

[55] Universia España, «Por qué estudiar Ingeniería en Tecnologías de Telecomunicación» [En línea]. Available: http://noticias.universia.es/educacion/noticia/2015/06/30/1127468/estudiar-ingenieria-tecnologias-telecomunicacion.html.

[56] Todo Nóminas, «EL MUNDO DE LAS NÓMINAS A TU ALCANCE» [En línea]. Disponible en: http://todonominas.blogspot.com.es/2011/06/base-de-cotizacion-parte-iii.html.

[57] Psinai, «Materiales directos e indirectos» [En línea]. Disponible en: https://psinai.wordpress.com/2013/03/03/materiales-directos-e-indirectos/.

[58] Economipedia, «Amortización contable lineal» [En línea]. Disponible en: http://economipedia.com/definiciones/amortizacion-contable-lineal.html.

[59] KAPPOS, George, et al. An Empirical Analysis of Anonymity in Zcash. *arXiv preprint arXiv:1805.03180*, 2018.

[60] BIRYUKOV, Alex; FEHER, Daniel. Deanonymization of Hidden Transactions in Zcash. 2018.

[61] SASSON, Eli Ben, et al. Zerocash: Decentralized anonymous payments from bitcoin. En*2014 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2014. p. 459-474.

[62]Bitcoin coreclient, [En línea]. Disponible en:https://bitcoin.org/en/bitcoin-core/

[63] Wallet encryption, [En línea]. Disponible en: https://en.bitcoin.it/wiki/Wallet_encryption

[64] Cómo asegurar tu monedero, [En línea] - Disponible en: https://es.bitcoin.it/wiki/C%C3%B3mo_asegurar_su_monedero

[65] Kaminsky,D.[2011]. "BlackOpsofTCP/IPPresentation. [En línea] - Disponible en:

http://dankaminsky.com/2011/08/05/bo2k11/

[66] Bifurcación de la cadena de bloques [En línea] – Disponible en: https://bitcoinforks.io/

[67] Compra venta de Bitcoins. [En línea] – Disponible en: https://localbitcoins.com/es/

[68] MOSER, Malte; BOHME, Rainer; BREUKER, Dominic. Aninquiryintomoneylaunderingtools in the Bitcoin ecosystem. En *eCrimeResearchers Summit (eCRS), 2013*. IEEE, 2013. p. 1-14.

[69] Ley 25/2007, [En línea] – Disponible en: https://www.boe.es/ buscar/act.php?id=BOE-A-2007-18243

[70] Blockchainsql, [En línea] – Disponible en: http://blockchainsql.io/